Tibor Lakner

3G-ETÄTUKIASEMA

Tietotekniikan koulutusohjelma

2015

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

3G-ETÄTUKIASEMA

Lakner, Tibor
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Joulukuu 2015
Ohjaaja: Aromaa, Juha, DI
Sivumäärä: 50
Liitteitä: 2

Asiasanat: 3G-tekniikka, lähiverkot, matkaviestinverkot, tietoturva, tukiasemat

---

Mobiiliverkkojen tekniikoiden opetus on Satakunnan ammattikorkeakoulun tietoliikenneopetuksen kiinnostavin osa. Opetusympäristön keskipisteenä oleva NGN-laboratorion toiminta herättää kiinnostusta laajalti ja sen esittämiseen tarvitaan liikuteltavaa 3G-tukiasemaa. Matkapuhelinverkkojen kehityksen myötä siirtoyhteydet ovat yhä enenevässä määrin IP-pohjaisia koskien myös tukiasemia. Kaupallisissa toteutuksissa laitteiden välinen kytkentä on joko suoralinkki tai verkko-operaattorin oma IP-verkko, mutta opetuskäytössä on sekä edullista että helposti toteuttavaa käyttää maailman suurinta IP-verkkoa, Internetiä.

Tässä työssä tutkittiin, millä tavalla merkinantosignaali ja käyttäjädata siirtyvät tukiaseman ja radioverkko-ohjaimen välisissä yhteyksissä, jos tiedonsiirrossa käytetään IP-verkkoja. Tunnelointimenetelmä tarjoaa mahdollisuutta yhdistää verkkoja saumattomiksi kokonaisuuksiksi ja sen lisäksi salata tietoliikennettä tietoturvan varmistamiseksi. Ennen varsinaista asennustyötä selvitettiin NGN-laboratorion UMTS-radioverkon laitteiden kytkennän yksityiskohtia. Erityisen tarkasti tutkittiin Savonia ammattikorkeakoulussa sijaitsevan 3G-tukiaseman VPN-yhteyttä, joka on rakennettu NGN-laboratorion pfSense-palvelimen kautta.

Tutkimusten jälkeen päätettiin asentaa VPN-tunneli, pfSense-palvelimien kautta, käyttämällä avoimeen lähdekoodiin perustuvaa openVPN-ohjelmistoa. Valittiin asiakas-palvelinarkkitehtuuri, joka sopii parhaiten siirrettävän etätukiaseman kytkemiseen. Sen symmetrisen salaustekniikka on ns. jaettu avaimen menetelmä, joka käyttää 256-bittisen AES-salausta ja autentikointi tapahtuu 160-bittisen SHA1-tiivistearvon avulla. Testikäytön jälkeen ratkaisu todettiin oikein helppokäyttöiseksi, koska se ei tarvitse mitään käyttäjätunnuksia tai salasanoja tunnelin avaamiseen. Konfiguroinnin jälkeen VPN-tunneli on käytettävissä heti, kun verkkokaapelit kytketty ja pfSense-palvelin käynnistyy.

3G REMOTE BASE STATION

Lakner, Tibor
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Programme in Information Technology
December 2015
Supervisor: Aromaa, Juha, MSc
Number of pages: 50
Appendices: 2

Keywords: 3G technology, local area networks, mobile communication networks, data security, base stations

---

The teaching of mobile network technologies is the most interesting part of telecommunications studies at Satakunta University of Applied Sciences. The NGN laboratory, which is the focal point of the learning environment, interests many widely and its presentation requires a movable 3G base station. Through the development of mobile networks transport links have become more and more IP based, including base stations. In commercial service the connection between devices is either a direct link or a network operator's own IP network, but for teaching purposes it is both inexpensive and achievable to use the world's largest IP network, the Internet.

The way how signalling and traffic are transferred in connections between the base station and the radio network controller in case of IP networks was examined in this thesis. The tunneling protocol makes possible the combining of networks into seamless units and additionally hide telecommunication to ensure information security. Before the actual installation the details of connection of equipment in NGN laboratory's UMTS radio network were investigated. Special attention was given to the 3G base station's VPN connection, located at Savonia University of Applied Sciences, which was built through the NGN laboratory's pfSense server.

After the analysis the decision was made to install a VPN tunnel through the pfSense servers by using the open source based openVPN software. A client server architecture best suited for connecting a transferrable remote base station was chosen. The model's symmetrical key encryption is the so called shared-key method, which uses a 256-bit AES encryption and authentication takes place with the help of the 160-bit SHA1 cryptographic hash values. After testing the solution was found to be extremely user friendly, on the account of how it does not require any usernames or passwords to open the tunnel. Following the configuration the VPN tunnel is available for use as soon as the network cables have been connected and the pfSense server is online.

SISÄLLYS

LYHENTEET

1G	1st generation
2G	2nd generation
3DES	Triple Data Encryption Algorithm
3G	3rd generation
3GPP	3rd Generation Partnership Project
5GPPP	5G Infrastructure Public Private Partnership
AES	Advanced Encryption Standard
AES	Advanced Encryption Standard
AMR	Adaptive multirate
ATM	Asynchronous Transfer Mode
AuC	Authentication Centre
BSS	Base Station Subsystem
CESoPSN	Circuit Emulation Service over Packet-Switched Network
CN	Core Network
CoMP	Coordinated Multi Point operation
CS	Circuit Switched
CSoHSPA	Circuit-Switched over HSPA
D2D	Device-to-Device
DeNB	Donor eNodeB
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DL	Downlink
DSA	Digital Signature Algorithm
EDGE	Enhanced Data rates for GSM Evolution
EGPRS	Enhanced GPRS
EIR	Equipment Identity Register
eMBMS	Evolved Multimedia Broadcast Multicast Service
eNB	Evolved Node B
EPC	Evolved Packet Core
EPS	Evolved Packet System
ESP	Encapsulating Security Payload
Ethernet	yleisin lähiverkkotekniikka, IEEE 802.3

E-UTRAN	Evolved Universal Terrestrial Access Network
FBMC	Filter-Bank Multi-Carrier
GERAN	GSM/EDGE Radio Access Network
GFDM	Generalized Frequency-Division Multiplexing
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSDPA	High Speed Downlink Packet Access
HSS	Home Subscriber Server
HSUPA	High Speed Uplink Packet Access
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Subsystem
IMT	International Mobile Telecommunications
IMT-A	IMT-Advanced
IP	Internet Protocol
IPSec	IP Security Architecture
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunications Union
LAN	Local Area Network
LTE	Long Term Evolution
LTE-A	LTE-Advanced
MAC-address	Media Access Control address
MBMS	Multimedia Broadcast Multicast Service
MGW	Media Gateway
MIMO	Multiple Input Multiple Output
MSC	Mobile Switching Center
MSC-S	Mobile Switching Center Server
MSS	Mobile Switching center Server
NGN	New Generation Networks
NMT	Nordic Mobile Telephony
NSN	Nokia Siemens Networks
OFDMA	Orthogonal Frequency Division Multiple Access

OSI-model	Open Systems Interconnection model
PCI	Peripheral Component Interconnect
PCM	Pulse-code Modulation
PDH	Plesiochronous Digital Hierarchy
PIN	Personal Identification Number
ProSe	Proximity Services
PS	Packet Switched
PTP	Precision Time Protocol
QAM	Quadrature Amplitude Modulation
RAN	Radio Access Network
RNC	Radio Network Controller
RSA	Rivest-Shamir-Adleman cryptosystem
S/N	Signal to Noise ratio
SAMK	Satakunnan ammattikorkeakoulu
SCTP	Stream Control Transmission Protocol
SHA1	Secure Hash Algorithm 1
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SON	Self Organising Networks
SS7	Signalling System no.7
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDM	Time-division Multiplexing
TLS	Transport Layer Security
TM	Transmission Modes
ToP	Timing over Packet
TX div.	Transmission diversity
UDP	User Datagram Protocol
UE	User Equipment
UFMC	Universal Filtered Multi-Carrier
UL	Uplink
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register

VLR	Visitor Location Register
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WiMax	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

1 JOHDANTO

Satakunnan ammattikorkeakoulun (SAMK) tietoliikenneopetuksen matkapuhelinlaboratorio sijaitsee Porin Tiedepuisto B kampuksessa. Sitä kutsutaan myös NGN-laboratorioksi (New Generation Networks) johtuen siitä, että yhä enenevässä määrin laitteiston kytkennöissä käytetään IP- (Internet Protocol) verkkoja. Maailmassa ainutlaatuinen mobiiliverkkojen opetus- ja opiskeluympäristö on rakennettu eri valmistajien mm. Ericsson ja NSN (Nokia Siemens Networks) laitteista. Samalla tavalla kuin kaupalliset verkko-operaattoritkin, laboratorion verkko tarjoaa uusimpia palveluita ja tekniikoita käyttäjien päätelaitteille. Laitteet toimivat SAMKin omilla SIM- (Subscriber Identity Module) korteilla, tietenkin hyvin rajoitetulla alueella. Matkapuhelinlaboratorion toiminta herättää kiinnostusta sekä kotimaassa, että kansainvälisestikin. Vaihto-oppilaita tulee jatkuvasti kaikkialta maailmasta kokemaan mobiiliverkkojen ylläpitoa, minkä lisäksi mobiiliverkon etäkäyttöäkin on toteutettu. Useassa korkeakoulussa, sekä Suomessa että muualla Euroopassa, 2G- (2nd generation) ja 3G- (3rd generation) tukiasemia on kytketty Internetin kautta VPN- (Virtual Private Network) tunnelin avulla laboratorion verkkoon. SAMK aikoo laajentaa opetustoimintaansa edelleen mobiilitekniikasta muiden toimijoiden ja partnereiden suuntaan, mutta kiinteästi asennettu laitteisto ei ole aina mahdollista. Laitteita ei ole tarpeeksi halukkaisiin nähden, lisäksi tarpeet voivat olla lyhytaikaisia, muutaman viikon projektityön tai jopa yhden päivän esittelyn vuoksi.

Tarvitaan liikuteltava tukiasemalaitteisto, joka on toimintavalmis paikasta riippumatta. Tämän opinnäytetyön tarkoitus oli suunnitella ja asentaa sellainen VPN-yhteys tukiasemalle, joka toimii paikassa kuin paikassa, kunhan siellä on Internet-yhteys. Toisin kuin 2G-tekniikassa, jossa tukiaseman yhteydet ovat TDM (Time-division multiplexing), eli aikajakomodulaatiopohjaisia ja tukiaseman kytkeminen Internetin IP-verkkoihin vaatii VPN-tekniikan lisäksi erikoismodeemin, CESoPSN- (Circuit Emulation Service over Packet-Switched Network) protokollan ominaisuuksilla, 3G-tukiaseman voi yhdistää radioverkko-ohjaimeen (RNC, Radio Network Controller) Ethernet- (yleisin lähiverkkotekniikka, IEEE 802.3) kaapelilla ja sitä voi tarvittaessa tunneloida Internetin kautta suhteellisen vaivattomasti. Työn suunnittelu vaatii kuitenkin perehtymistä erilaisiin VPN-ratkaisuihin, sekä SAMKin NGN-laboratorion

mobiiliverkon tuntemusta siltä osin, joka koskee tukiaseman ja radioverkko-ohjaimen toimintaa. Erityisesti toiminnassa olevia etätukiasemien, kuten Savonia AMK:n (ammattikorkeakoulu) VPN-tunnelointia on syytä tutkia, jotta tulevan liikuteltavan tukiaseman verkkoyhteys mahdollisesti sopii lisättäväksi nykyiseen VPN-palvelimeen.

2 MATKAPUHELINVERKKOJEN KEHITYS

Matkapuhelinverkkojen kehityksen ensimmäinen analoginen järjestelmä (1G, 1st generation) kehitettiin 1980-luvuilla. Euroopassa sitä kutsuttiin NMT- (Nordic Mobile Telephone) järjestelmäksi. Seuraava kehitysaskel oli, kun toisen sukupolven verkkotekniikka (2G) saapui 80-luvun lopussa, tuomalla mukanaan digitaalisen tekniikan etuja, joka mahdollistaa tiedonsiirtopalvelun lisäksi myös muita palveluita. Se on GSM (Global System for Mobile communications), maailmanlaajuinen mobiili kommunikointijärjestelmä, joka onnistui tarjoamaan asiakkaille verkkovierailun, eli käyttämään puhe- ja muita palveluita, käsipuhelimen ja siihen liitetyn SIM-kortin avulla, paikasta riippumatta myös matkustaessa vieraissa maissa. [4]

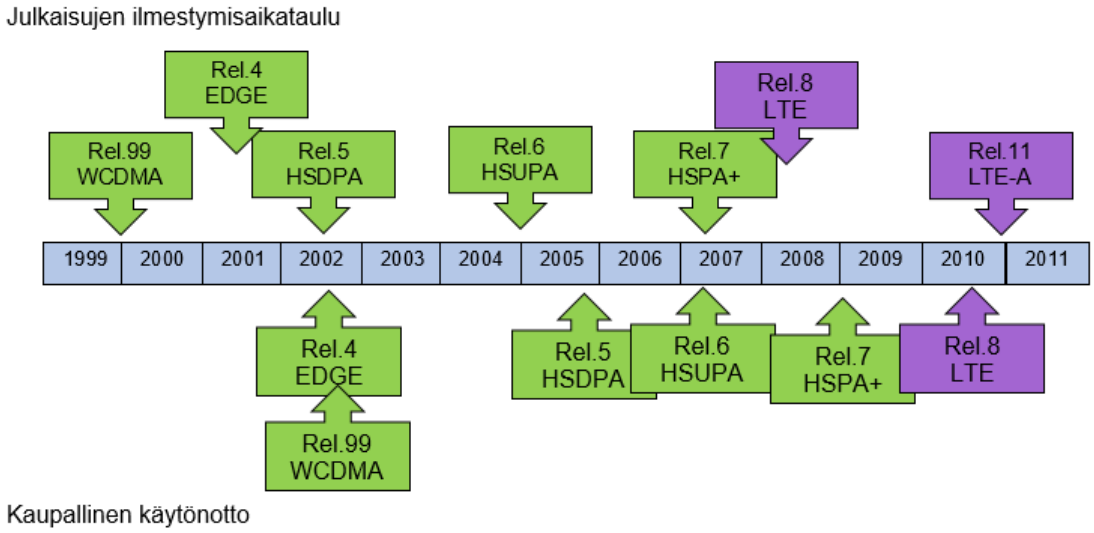
Vuonna 1991 ensimmäisenä maailmassa avattiin kaupallinen GSM-verkko Suomessa, Radiolinja verkko-operaattorin toimesta. Nopeasti GSM-järjestelmästä tuli yksi maailman tärkeimpiä matkapuhelinverkkoja, niiden yhteenlaskettu käyttäjäkunta ylitti miljardin vuonna 2005. [9]

2.1 Standardointi

3G-standardointityöryhmä 3GPP (3rd Generation Partnership Project) perustettiin joulukuussa 1988, kehittämään matkapuhelinverkkoja Euroopassa. Työryhmän tarkoitus oli, että verkkokehityksen tekniikoita standardisoidaan ja dokumentoidaan. [8]

Tämä kehitystyö on jatkuvaa. Aina kun yksi vaihe, jota kutsutaan julkaisuksi (engl. release), on saatu päätöksiin, se jäädytetään (engl. frozen) ja se ei enää muutu. Sen jälkeen laitevalmistajat ja palveluntarjoajat ottavat sen käyttöönsä. Julkaisun jäädyttäminen ja kaupallisen käytön alkamisen välissä voi olla viivettä jopa useita vuosia riippuen markkinatilanteesta. Esimerkkinä voisin mainita UMTS (Universal Mobile Telecommunications System) matkapuhelinteknologian julkaisun Rel.99. Se jäädytettiin 1999, mutta kaupallinen käyttö alkoi vasta vuonna 2002. Vielä enemmän ovat viivästyneet HSDPA:n (High-Speed Downlink Packet Access) ja HSUPA:n (High-Speed Uplink Packet Access) standardit, jotka olivat valmiina jo vuosina 2002 ja

2004, mutta kaupallinen levittäminen oli vuosina 2005 ja 2007. Vastaavia aikaeroja voidaan havaita seuraavasta kuvasta (Kuva 1). [7]



Kuva 1. Matkapuhelinverkkojen standardien julkaisuajat

2.2 3G-arkkitehtuurin kehitysvaiheet

Kehitys kohti kolmannen sukupolven 3G-verkkoja ei ollut mutkatonta. GSM-verkon käyttäjille tarjottiin ensin pakettidatan tiedonsiirtopalvelua (GPRS, General packet radio service), sitten laajennettua siirtokaistaa (EDGE, Enhanced Data Rates for GSM Evolution) (Kuva 2). Tämä oli välttämätöntä ennen seuraavaa askelta uuteen tekniikkaan, koska silloin vuoden 2002 joulukuussa maailmassa oli yli 780 miljoona GSM-tilaaja, mikä oli 71 % kaikista matkapuhelinten käyttäjistä. [4]

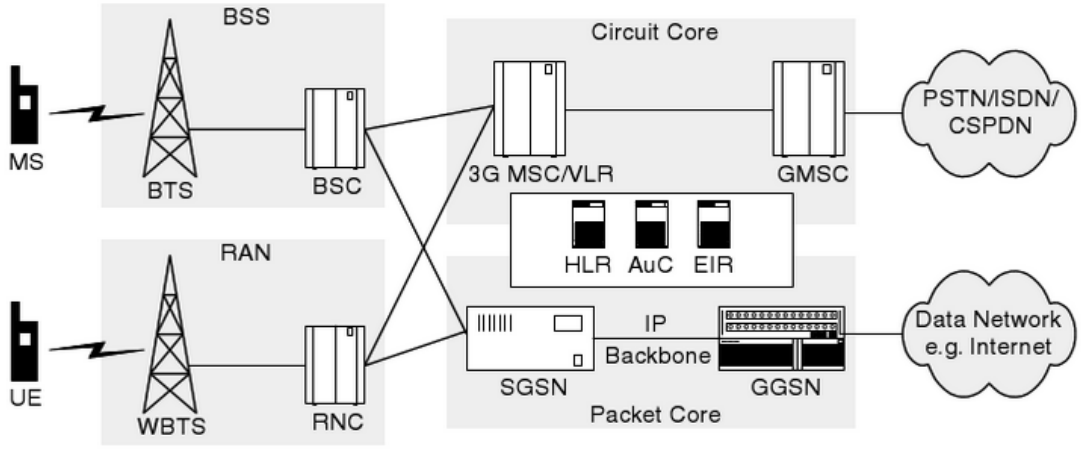
Kuva 2. Matkapuhelinverkkojen kehitys kohti 3G:tä

UMTS- (Universal Mobile Telecommunications System) verkkotekniikan käyttöönotto on tuonut ennen kaikkea radiolinkkiin liittyviä uudistuksia, joiden avulla tiedonsiirtonopeuden kehitys on saanut uutta vauhtia. [4]

2.2.1 Release 99 – Release 4

UMTS-järjestelmän ensimmäisen spesifikaation julkisti 3GPP työryhmä, se oli Release 99. Siinä oli melko vahva ‘GSM läsnäolo’, johtuen siitä, että ensinnäkin UMTS-järjestelmän pitää olla taaksepäin yhteensopiva olemassa olevan GSM-järjestelmän kanssa, toisaalta GSM:n ja UMTS:n pitää tulla toimeen keskenään. Kun GSM:n pakettidatapalveluja ja sen mukana tulevia lisäpalveluita tarjotaan myös UMTS-verkon asiakkaille, se tuo mukanaan ilmiselviä valintoja rakentaessa UMTS-järjestelmän runko-verkkoja (CN, Core Network). Edellä mainitut vaatimukset selvittävät sitä, miksi runkoverkko on toiminnallisesti jaettu kahteen, piirikytkentäiseen ja pakettikytkentäiseen osaan. [9]

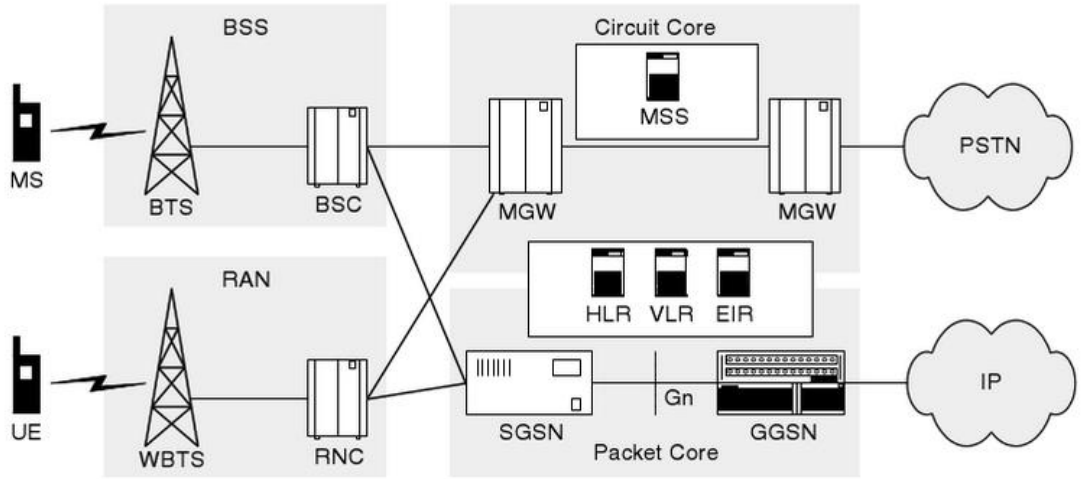
3G-verkkojen ensimmäisen sukupolven, eli Release 99 mukaisen UMTS-verkon topologian kytkentäkaavio on seuraavassa kuvassa (Kuva 3).



Kuva 3. UMTS Release 99 verkkotopologia [4]

Release 4 sisältää merkittäviä muutoksia runkoverkon piirikytkentäisessä osassa, sen takia, että käyttäjädatan merkinanto erotetaan sen tietovuosta. Myös multimedian käsittelyyn lisättiin sopivia mekanismeja. MSC/VLR (Mobile Switching Center, Visitor Location Register) serveri on jaettu MSC-S (Mobile Switching Center Server) palve-

limeksi ja MGW (Media Gateway) yhdyskäytäväksi. MSC-palvelin, jonka lyhenne MSC-S tai MSS, huolehtii päätelaitteen yhteyden toimivuuden sekä liikkuvuuden hallinnasta ja sisältää myös VLR-palvelimen. Kytkentä tapahtuu MGW:n kautta jolla on myös toimintoja verkkojen yhteistyötä varten, esim. transkooderi, kaikujen estolaite sekä MGW:ssä sijaitsevat modeemit. Verkon rakenteesta riippuen MGW:ssä voi olla paketti-piiri muunnosten suorittavia osia, joita tarvitaan VoIP- (Voice over IP) puhelujen käsittelyssä. MSC ja MGW palvelinten jakaminen ei tapahdu yksi-yhteen, vaan tarpeellisuudesta riippuen kummastakin voi olla useita yksiköitä. Verkkoarkkitehtuuri Release 4 mukaisesti (Kuva 4). [9]

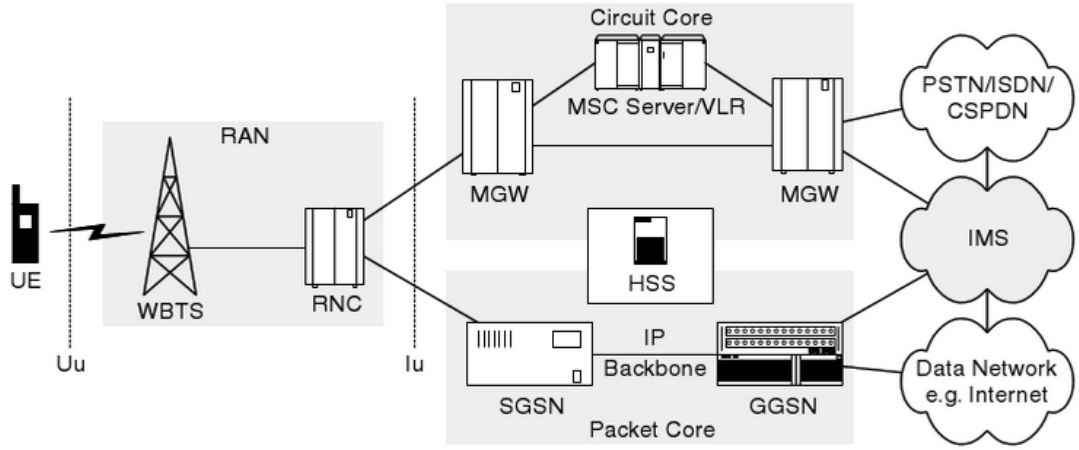


Kuva 4. UMTS Release 4 arkkitehtuuri [4]

2.2.2 Release 5

3GPP R5 julkaisu on tärkeä merkkipaalu verkkojen kehityksessä, koska sen aikomus oli lisätä siirtoyhteyksien toteutuksiin mahdollisimman paljon IP-tekniikkaa. Tästä johtuen Release 5 UMTS-verkko sai ’kaikki IP-verkko’ (engl. ‘All IP’) nimen. IP-protokollaa tullaan käyttämään sekä merkinantoon että käyttäjädatan kuljettamiseen verkkoelementtien välissä. Julkaisu sisältää uuden multimedia alijärjestelmäelementin, joka kutsutaan IMSiksi (IP Multimedia Subsystem). Se on tarkoin määritelty yhdenmukainen kokonaisuus. Yksi tärkeimmistä ominaisuuksista on VoIP-puheluiden hallinta UMTS-verkkojen välissä. Matkapuhelinverkkojen arkkitehtuurissa, sopusoinnussa Release 5 spesifikaation kanssa, siirtoprotokolla pakettidataverkoissa on päästä päähän IP. [9]

Verkon kehityksessä on edistytty käyttämään hyväksi laitteiden suorituskykyjen valtavaa kasvua. Tästä johtuen HLR- (Home Location Register), VLR- (Visitor Location Register) ja EIR- (Equipment Identity Register) palvelimet on yhdistetty yhdeksi HLR-alijärjestelmäksi, jota kutsutaan tästä eteenpäin HSS:ksi (Home Subscriber Server). Huomion arvoista on myös, että R5:n mukaisissa verkoissa piirikytkentäinen runkoverkko (engl. CN CS domain) on edelleen tarjolla niin kauan kuin niiden palveluita tarvitaan. Verkko-operaattorit käyttävät R4 piirikytkentäisiä palveluita sen sijaan, että käyttäisivät R5:n mukaista IMS-arkkitehtuuria. Tällä tavalla toteutuu asteittainen migraatio kaikkiin IP-verkkoihin ja verkkopalveluita tarjotaan häiriöittä käyttäjille. Joitakin äänipuheluita käsitellään piirikytkentäisessä verkossa, vaikka muita esim. videopuheluita siirretään IMSin kautta. Topologiakuva migraatiosta on seuraavassa kuvassa (Kuva 5). [4]

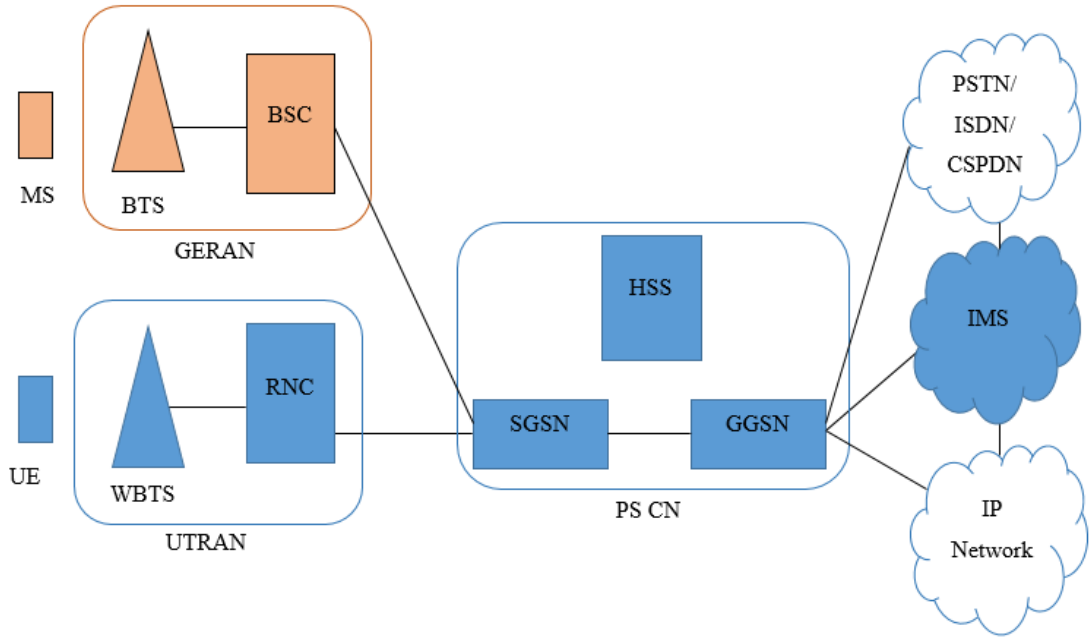


Kuva 5. Verkon arkkitehtuuri siirtymisessä R4:stä R5:een [4]

Tietoliikenne on aina pakettikytkentäistä tässä R5 julkaisussa. Kehityksen painopiste on paketti-toimialueella (engl. PS domain), joka laajenee IMSin toiminnoilla. Muutokset R4:n ja R5:n välissä eivät ole näkyviä loppukäyttäjille. UTRAN- (UMTS Terrestrial Radio Access Network) radioverkko toimii samalla tavalla kuin ennenkin. Liityntäverkon (engl. Access Network) siirtoteknologia on ATM:n (Asynchronous Transfer Mode) sijaan IP. UTRAN-verkon rinnalla kehitetty uusi nopeampi GSM-radioliityntäverkko GSM BSS (Base Station Subsystem), jonka nimi on GERAN (GSM/EDGE Radio Access Network), kytketään paitsi paketti- myös piirikytkentäiseen runkoverkkoon. Jos operaattorilla on IMS-palveluja käytettävissään, piirikyt-

kentäistä runkoverkon toimialuetta ei tarvitse enää paljon mihinkään. Tämä oli suuri askel VoIP-puhelujen kehityksessä. [9]

Edellisen kappaleen ratkaisussa uusi verkkotopologia palvelee 3G-verkon käyttäjiä puheyhteyksissä vanhan tapaan, piirikytkentäisen runkoverkon kautta. Vanhempien GSM-päätelaitteiden käyttäjiä varten, joilla ei ole mahdollisuutta käyttää 3G-radiorajapintaa, yhteensopivuuden varmistamiseksi pitää edelleen olla 2G-radioverkko. Tähän sopiva ratkaisu on edistynyt pakettidatapalvelu EGPRS (Enhanced GPRS), jota tarjotaan GERANin kautta. Tässä tapauksessa myös puheyhteyksiä ohjataan, samalla tavalla kuin 3G-puheluita, pakettikytkentäisen runkoverkon välityksellä (Kuva 6).



Kuva 6. GSM-asiakkaiden kytkentä pakettirunkoverkon kautta

IP-verkkoja on kahdenlaisia. Alkuperäinen IPv4 (Internet Protocol version 4), joka on edelleen käytössä ja uusi IPv6 (Internet Protocol version 6), jonka käyttö laajenee koko ajan. 3GPP R5 julkaisun mukaan UTRAN-verkon IP-siirtoyhteyksissä IPv6 on pakollinen ja IPv4 on valinnainen tapa reitittää paketteja. Tästä johtuen molempien yhteyskäytäntöjen rinnakkaiskäyttö (engl. Dual Stack) on ehdottomasti suositeltua. [10]

2.2.3 Release 6-7

R6 on laajennus edellisestä 3GPP:n julkaisusta R5:stä, joka tuo mobiilikäyttäjille täydellisiä 3G-kokemuksia. Se sisältää lukuisia uusia ominaisuuksia. Radioverkon nopeutta on lisätty merkittävästi uusilla HSUPA (High Speed Uplink Packet Access) ja HSDPA (High Speed Downlink Packet Access) tekniikoilla sekä UL- (Uplink,) että DL- (Downlink) suuntaan. IMSin toinen vaihe tekee WLAN- (Wireless Local Area Network) verkkojen kanssa yhteistyötä tarvittaessa. Se on laajennettu SIP- (Session Initiation Protocol) tekniikalla ja sen avulla palvelupohjaisia Internet-sovelluksia voidaan tarjota asiakkaille. Multimedia levitys- (engl. broadcast) ja ryhmäsanomien (engl. multicast) käyttö (MBMS, Multi Broadcast Multicast Services) kaksisuuntaisella symmetrisellä huippunopealla datayhteydellä parantaa videoneuvottelujen sujuvuutta, sekä mahdollistaa VoIP-puhelintekniikan käytön mobiililaitteellakin. [9]

Release 7:n uudistuksia ovat tiedonsiirtonopeuksien kasvaminen parannetulla tekniikalla HSPA+, suurimmat teoreettiset nopeudet ovat latauksessa 28 Mbps ja paluusuunnassa 11,5 Mbps. Merkittävä kehitys on myös MIMO- (Multiple Input Multiple Output) tekniikan käytönotto. MIMO:ssa käytetään päätelaitteen ja tukiaseman välissä useita antenneja tilanteesta riippuen. Yhtenä esimerkkinä voidaan mainita 2x2 MIMO, joka tarkoittaa kahta antennia sekä tukiaseman että mobiililaitteen (UE, User Equipment) päässä. CSoHSPA- (Circuit-Switched over HSPA) protokollan käyttö on standardoitu 3GPP R7:ssä sallimaan piirikytkentäisiä puheluita HSPA:n radiorajapinnan kautta vaikuttamatta millään tavalla runkoverkkoon. Toisin sanoen piirikytkentäisessä runkoverkossa käytetään samaa MSC:tä kuin aikanaan R99:n mukaisissa UMTS-verkoissa AMR- (Adaptive multirate) puheluissa. [11]

2.3 4G-arkkitehtuurin kehitysvaiheet

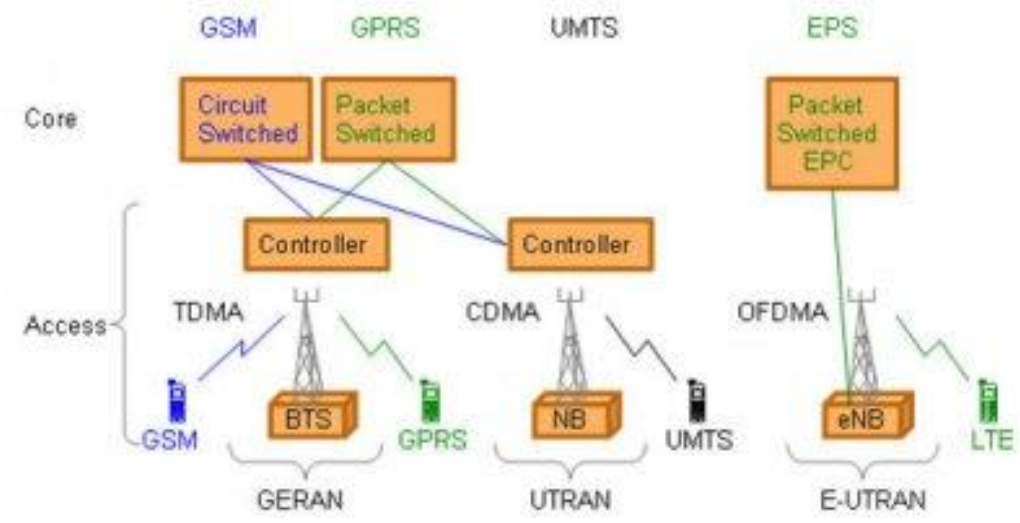
2.3.1 LTE Release 8-9

Seuraavaan sukupolven mobiilitekniikka alkoi sen standardien kehityksellä. 3GPP jäädytti Release 8 julkaisun suositukset joulukuussa 2008, se oli hyvä pohja LTE- (Long Term Evolution) laitteiden ensimmäisellä aallolle. [12]

LTE:n suunnittelun motivaatio ja määränpää oli selvä, sen kehitys alkoi jo vuonna 2004, vaikka silloin sen edeltäjän, HSDPA:n levitys ei ollut edes alkanut. Seuraavan radiojärjestelmän suunnittelutyön aloitus oli välttämätöntä, koska suunnittelusta levitykseen ja käytönottoon saakka kuluu yli viisi vuotta. Kunniahimoisia tavoitteita hankkeelle olivat mm. ne, että tiedonsiirtonopeuksien pitää ylittää 100 Mbps DL ja 50 Mbps UL arvot, verkon toiminta on optimoitu nimenomaan pakettikytkentäiselle yhteyksille, pitää olla korkeatasoinen liikuteltavuus ja tietoturva, sekä päätelaitteen tehokas virrankäyttö on optimoitu. [13]

LTE, joka kutsutaan myös nimellä E-UTRAN (Evolved Universal Terrestrial Access Network), on kehittänyt pakettijärjestelmän, ts. EPS- (Evolved Packet System) järjestelmän radioliityntäverkkoa. EPS on puhtaasti IP-pohjainen, paitsi reaaliaikaisia palveluja myös tietoliikennepalveluja kuljettaa IP-protokolla. Mobiililaitteelle varataan IP-osoite, jos se on kytketty päälle ja osoite vapautuu, kun se sammutetaan. LTE on uusi verkkoonpääsyratkaisu, joka perustuu OFDMA- (Orthogonal Frequency Division Multiple Access) modulaation ja enintään 64QAM- (Quadrature Amplitude Modulation) koodaukseen, käyttämällä peräti 20 MHz kaistaleveyttä sekä MIMO-tekniikkaa maksimissaan 4x4, saavutetaan ennenkuulumattomia nopeuksia. Korkeimman siirtokanavan teoreettinen huippunopeus on 75 Mbps yhteydessä ylöspäin (UL) ja 4x4 MIMO:n ansiosta latausnopeus (DL) voi olla jopa 300 Mbps. LTE radioliityntäverkko on yksinkertaisemmaksi kehittynyt tukiasemaverkko (eNB, Evolved Node B), jossa tukiasemat ovat keskenään yhteydessä X2-rajapinnan kautta, sekä jokainen niistä on suoraan kytketty matalassa arkkitehtuurissa (engl. flat architecture) S1-liittymällä runkoverkkoon (EPC, Evolved Packet Core). Radioverkko-ohjainta (RNC) ei ole enää, sen sijaan tukiasemalaitteistoon on integroitu lukuisia nopean

toiminnan vaativia funktioita. Verkkotopologian kehitystä esittää seuraava kuva (Kuva 7). Kuvassa piirikytkentäiset linkit ovat sinisellä ja IP-linkit vihreällä merkittynä. [12]



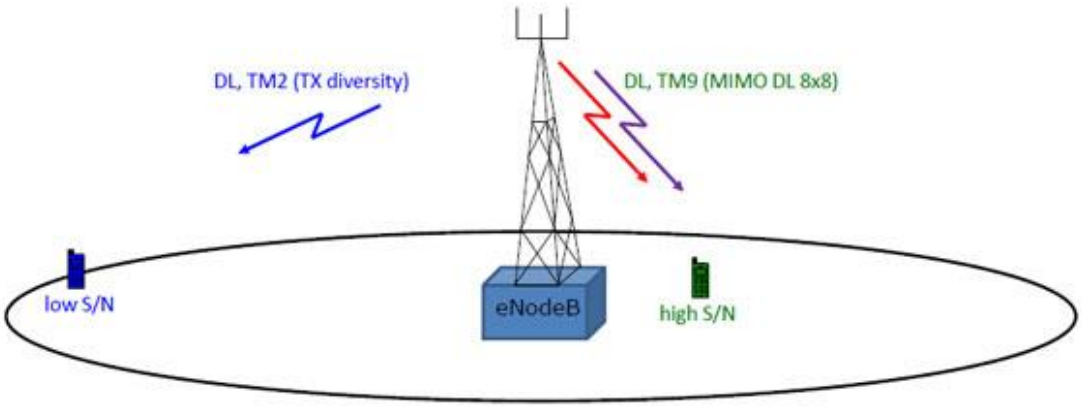
Kuva 7. Verkkoratkaisuja GSM:stä LTE:een [12]

Seuraava julkaisu R9, sisältää tärkeitä parannuksia päätelaitteen paikannuksessa, liittyen hätäpuheluvaatimuksiin. [7] Tämän lisäksi on jo käytössä oleva ns. Femtocell-käsite nyt täysin integroitu siihen, joka koskee pieniä, yksityiskäytössä olevia tukiasemia kotona tai toimistossa. Lisää parannuksia SON- (Self Organising Networks) tekniikassa, multimedian suoratoistopalvelussa (eMBMS, Evolved Multimedia Broadcast and Multicast Service), sekä uusia radiotaajuuksia on lisätty LTE:n toimintaan (esim. 800 MHz ja 1500 MHz). [15]

Ilmeisesti kaupallisesta syystä, verkko-operaattorit markkinoivat LTE-verkkoja 4G nimellä, vaikka se on määritelty ITU:n (International Telecommunications Union) standardissa vasta seuraavalle nopeammalle tekniikalle. Tästä yleisestä käytännöstä johtuen kansainvälinen tietoliikenne liitto (ITU) ilmoitti 6. joulukuuta 2010, että myös edistykselliset 3G-verkot, jotka ovat tämän tekniikan edelläkävijöitä, kuten LTE, WiMax (Worldwide Interoperability for Microwave Access) ja vastaavia muita (esim. HSDPA+) voidaan katsoa kuuluvaksi siihen. [16]

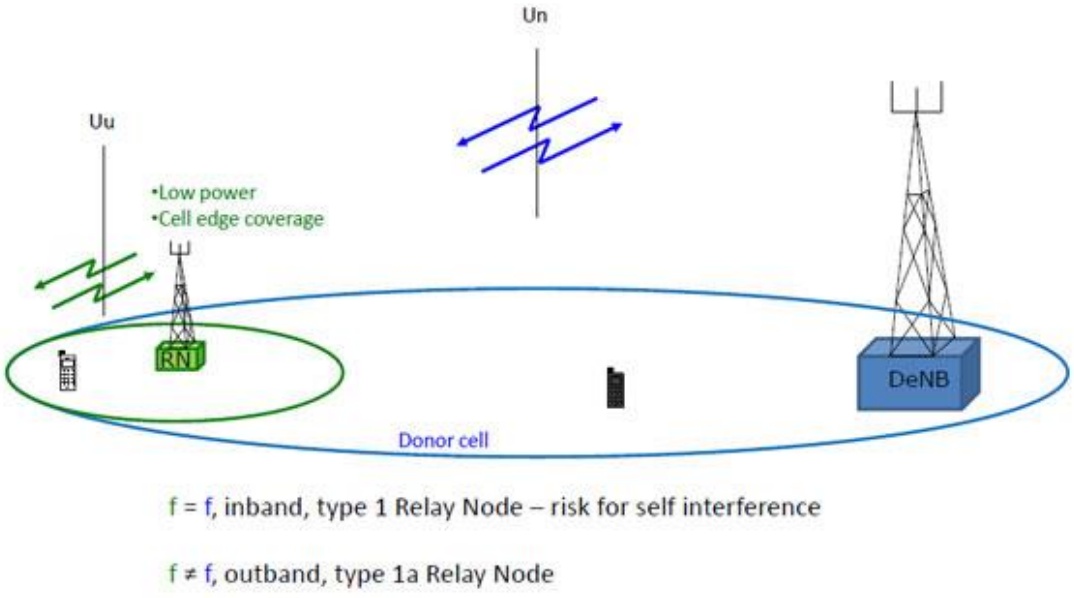
2.3.2 LTE-Advanced (4G)

Edistyneessä LTE:ssä, joka kutsutaan LTE-A:ksi (LTE-Advanced), polttopisteessä on korkeampi suorituskyky. Se voidaan saavuttaa 3GPP:n Release 10:n tarjoamalla korkeammalla bittinopeudella, joka samanaikaisesti täyttää täydellisesti ITU IMT-(International Mobile Telecommunications) Advanced, eli 4G:n vaatimukset. Verrattuna edellisiin nopeuksiin, nopeudet ovatkin uudessa luokassa. Käyttäjän latausnopeus (DL) on 3 Gpbs ja päätelaitteesta tukiasemalle (UL) on 1,5 Gbps. Radiokaistan tehokkuus on lähes kaksinkertaistunut R8:n 16 bps/Hz arvosta R10:n 30 bps/Hz arvoon. Solujen reuna-alueilla on myös parempi toimintakyky, esim. lataus (DL) 2x2 MIMO-tekniikalla vähintään 2,4 bps/Hz/solu. Toiminnallisista uutuuksista LTE-Advanced verkossa tärkein on kantoaaltokaistojen yhdistäminen (CA, Carrier Aggregation), tärkeitä uutuuksia ovat myös laajennettu moniantennitekniikka ja pienitehoinen releтukiasema (RN, Relay Nodes), joka ei ole kaapeloitu toiseen tukiasemaan, vaan radiorajapinnan kautta yhdistetty siihen. Moniantennitekniikan siirtotavoista (TM, Transmission Modes) LTE-A:ssa on tarjolla lataussuunnassa (DL) yhdeksän erilaista TM1-9, paluusuunnassa (UL) kaksi TM1-2, joista suurin osa oli jo mukana R8:ssa. Riippuen radiosignaalin kohinasta, joka mitataan signaalin ja häiriöiden suhteella (S/N, Signal to Noise ratio), siirtotavaksi solun reunalla käytetään esim. latauksseen MIMO-tavoista vakio TM2, eli TX div. (Transmission diversity) ja lähellä tukiasemaa TM9, joka käyttää peräti kahdeksaa antennia, eli 8x8 MIMO:a, mikäli päätelaite (UM) tukee sitä. Kuva 8 esittää niitä tilanteita. [14]



Kuva 8. Siirtotavan valinta riippuu signaalin laadusta MIMO vs. TX div. [14]

Reuna-alueiden heikkous vähenee merkittävästi ns. reletukiaseman (RN) avulla. Sen käyttötapa muistuttaa langattomien lähiverkkojen tukiasemia, jotka toimivat toistimena (engl. repeater). Niiden pystyttämiseen ei tarvitse olla kuituyhteydessä toiseen tukiasemaan, jonka nimi on DeNB, (Donor eNode B), sen sijan kommunikointi hoituu radiolinkin kautta. Lataussuunnassa RN ja siihen linkitetty päätelaite käyttävät samoja taajuuksia, mikä voi aiheuttaa haitallista interferenssiä reletukiasemassa. Reletukiaseman laitteistokytkentä on kuvassa (Kuva 9). [14]

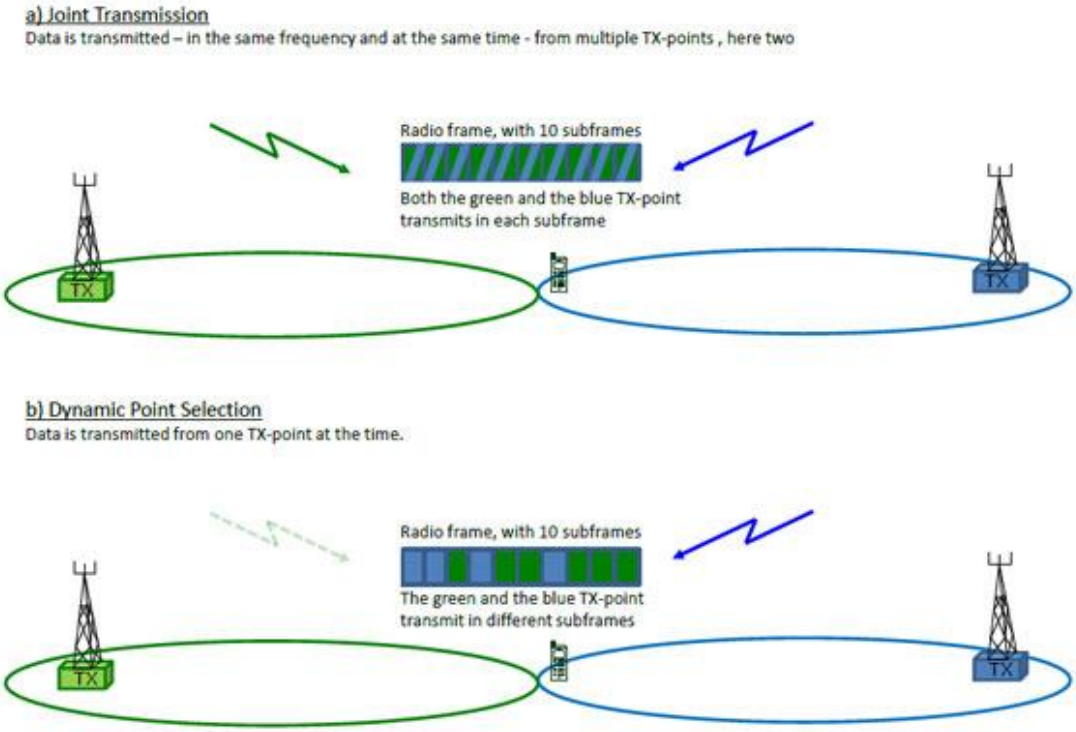


Kuva 9. Radiolinkin kautta kytketty reletukiasema [14]

Solujen reunojen radiolinkkiä parannetaan R11 alkaen myös uudella CoMP- (Coordinated Multi Point operation) tekniikalla, joka mahdollistaa mobiililaitteen olemaan samanaikaisesti yhteydessä kahteen tukiasemaan. Tiedonsiirto tukiasemilta voi tapahtua samanaikaisesti samalla taajuudella usealta tukiasemalta (engl. Joint Transmission) tai vuorotellen (engl. Dynamic Point Selection). Kuvassa (Kuva 10) on latausesimerkki CoMP:stä. [14]

Tämän hetken viimeiseksi suljettu suositus on 3GPP R12. Sen mukaan LTE-A ja HSPA+ saavat päivityksiä, mikä jatkaa kummankin tekniikan suorituskykyjen kehitystä. Verkon kapasiteetin kasvun lisäksi mobiililaitteiden käyttöaika latausten välissä suurenee parempien akkujen ja energiankulutuksen vähenemisen ansiosta. Yleisesti R12 mahdollistaa verkkokehityksen neljässä pääkohdassa LTE-A:n mukaisissa

toteutuksissa. Kehityksen painopisteessä ovat: LTE:n pienet solut ja heterogeeniset verkot, LTE:n moniantennitekniikka (MIMO), LTE:n paikallinen tietopalvelu (Pro-Se, Proximity Services), sekä LTE:n tuki kahdelle FDD ja TDD modulaatiolle, sisältäen myös kantoaaltojen yhdistämistä (CA). [21]



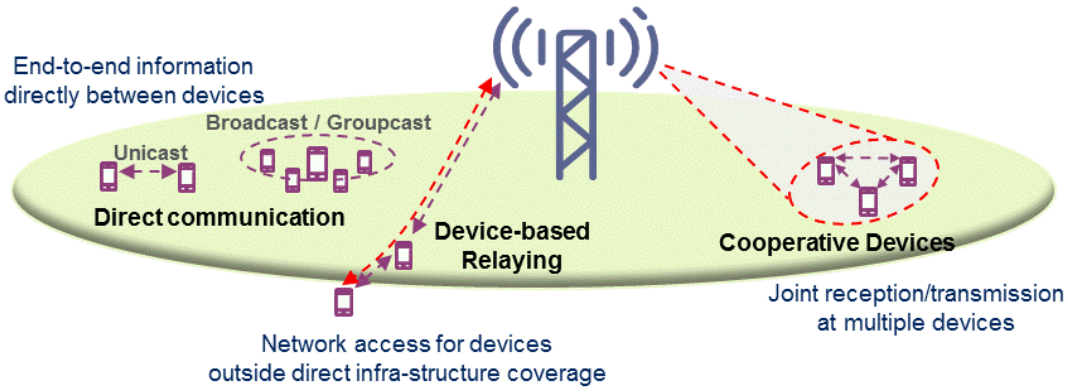
Kuva 10. Lataus (DL) monipistemenetelmällä (CoMP)

2.4 Jatkokehitysnäkymiä kohti 5G:tä

3GPP on julkistanut alustavan aikataulun seuraavan sukupolven, eli 5G-verkkotekniikan kehitystyöstä maaliskuussa 2015. 3G-projektityöryhmä esittää, että standardointityön viitekehys noudattaa kansainvälisen teleliikenneunionin (ITU) IMT-2020 työnimikkeen mukaista suunnitelmaa. Sen mukaan spesifikaatio pitää olla valmis lokakuussa 2020 mennessä. 5G-radioverkon toiminta ylittää 6 GHz taajuuden, koska jotkut kanavajaot vaativat sitä. [19]

Laajan selvityksen tulevaisuuden tekniikoista on julkaissut 4G Americas -niminen organisaatio, jonka jäseniä ovat tekniikkateollisuuden johtavat yritykset. Raportti esittää yksityiskohtaisesti mobiilikehityksen suunnitelman, jonka pohjana on myös

ITU:n IMT-2020 projekti. LTE:ssä radiorajapinnan toiminta perustuu OFDM modulaatioon sekä lataus- (DL) että paluusuunnassa, se on myös vahva kandidaatti 5G-verkkojen siirtotekniikaksi. Kuitenkin lukuisia muita mahdollisuuksia ovat mm. FBMC (Filter-Bank Multi-Carrier), UFMC (Universal Filtered Multi-Carrier), ja GFDM (Generalized Frequency-Division Multiplexing), joiden käyttöä myös harkitaan. Tulevaisuuden päätelaitteiden yhä paremman suorituskyvyn mahdollistaa niiden entistäkin tehokkaampi käyttö kommunikoinnissa, kun yhteydenpito tapahtuu suoraan laitteiden välillä. Tätä kutsutaan D2D (Device-to-Device) yhteydeksi. Sama tekniikka on standardisoitu, tosiaan paljon rajoitetummin, 3GPP R12 suosituksessa. Sen käyttö on ensisijaisesti viranomaisten keskeisessä yhteydenpidossa, sekä paljon yleisemmin kaupallisissa sovelluksissa, joissa käytetään D2D läheisten laitteiden havaitsemista. Kokonaisvaltaisessa langattomassa ratkaisussa välittömästä D2D-kommunikoinnista tulee yleinen integroitu apuväline (Kuva 11). [17]



Kuva 11. D2D langaton ratkaisu [17]

Helmikuussa 2013, Euroopan komissio perusti työryhmän nimellä 5GPPP (5G Infrastructure Public Private Partnership), jonka tehtävänä on kehittää tulevaisuuden Internet-verkkoa tulevalla 5G-tekniikalla vuoteen 2020. Kehityksen painopisteessä on suorituskykyinen maailmanlaajuinen verkko, joka on läsnä kaikkialla. Tavoitteena on, että projektityöryhmä aloittaa uuden 5G-tekniikan kaupallisen jakelun vuonna 2020. Tämä edellyttää, yhteistyössä 3GPPn kanssa, standardointityön tutkimuserän (engl. study item) aloittamista vuonna 2015. 3GPP jatkaa entisen tapaan verkkojen kehitystyötä sisällyttäen R14, R15, ja R16 julkaisuissa myös 5G:tä LTE-A:n rinnalla vuosina 2016–2020. 5GPPP työryhmän esitteen mukaan uuden sukupolven 5G on paljon enemmän, kuin pelkkää mobiililaajakaistaverkkoa. Sen pitää olla avaintekijä mahdollistamaan tulevaisuuden digitaalisen maailman, seuraavan sukupolven kaikki-

alla läsnä olevan huippunopean infrastruktuurin. Tässä ovat seuraavaksi konkreettisia lukuja siitä, kuinka korkeaa suorituskykyä ollaan tavoittelemassa:

- 1000-kertainen langatonverkkokapasiteetti verrattuna v. 2010
- 1000-kertaa enemmän kytkettyjä laitteita 1 M/km^2
- tiedonsiirron huippuarvo ≥ 10 Gbps
- käyttäjäkohtainen tiedonsiirtonopeus ≥ 50 Mbps
- 1/10-kertainen energiakulutus verrattuna v. 2010
- 1/5-kertainen päästä-päähän viive, yleisesti 5 ms
  ja kulkuvälineiden välissä ≤ 1 ms
- tiedonsiirron liikkuvuuden tuki ≥ 500 km/h
- suorituskyky palvella ≥ 20 miljardia terminaalia
- luotettavuus ≥ 99,999 %

[20]

3 TIETOTURVA

3.1 Matkapuhelinliikenteen tietoturva

Digitaalisessa matkapuhelintekniikassa on alusta asti huolehdittu järjestelmän tietoturvasta, mukaan lukien puhelujen salaaminen, tilaajan tunnistaminen sekä radiorajapinnan salaus. Jokaisella GSM-laiteella on oma yksilöllinen laitetunnus, eli IMEI- (International Mobile Equipment Identity) tunnus. Tilaajan tunnistaminen tapahtuu SIM-kortilla, joka sisältää suojausmahdollisuuden PIN- (Personal Identification Number) koodin avulla. GSM-verkko tarkistaa käyttäjän SIM-kortin oikeudet käyttämään verkkoa ennen puhelun aloittamista tunnistuskeskuksen avulla (AuC, Authentication Centre), joka on sijoitettu useimmiten HLR-palvelimeen. Salausavain määritellään tilaajasuhteen alussa ja se sijoitetaan paitsi SIM-kortille myös kotirekisteriin (HLR/AuC). Tilaajan todentaminen verkossa tapahtuu tietyn laskentakaavan mukaan niin, että salausavainta ei missä vaiheessa lähetetä radioverkossa. [22]

3.2 IP-verkon tietoturva

Tavallisesti IP-verkon tietoturva on heikkoa johtuen sen vahvuudesta, avoimuudesta ja joustavuudesta. Verkon ylläpitäjällä ja käyttäjällä on vastuu siitä, miten verkkoliikennettä suojataan ja tarvittaessa salataan. Tällä kertaa jätän käsittelemättä henkilökohtaisen tietokoneen virustorjunnan, koska se ei koske millään lailla matkapuhelinkeskuksen IP-liikennettä. Verkkojen suojauskeinojen tärkeämpiä osia ovat erilaiset palomuurit, joilla voidaan suodattaa liikennettä tarvittaessa. Palomuuria tarvitaan myös tunneloinnissa suojaamaan palvelimia, jotka yhdistävät palvelupisteiden lähiverkkoja Internetin yli. [18]

3.2.1 Tunnelointimenetelmät ja salaukset

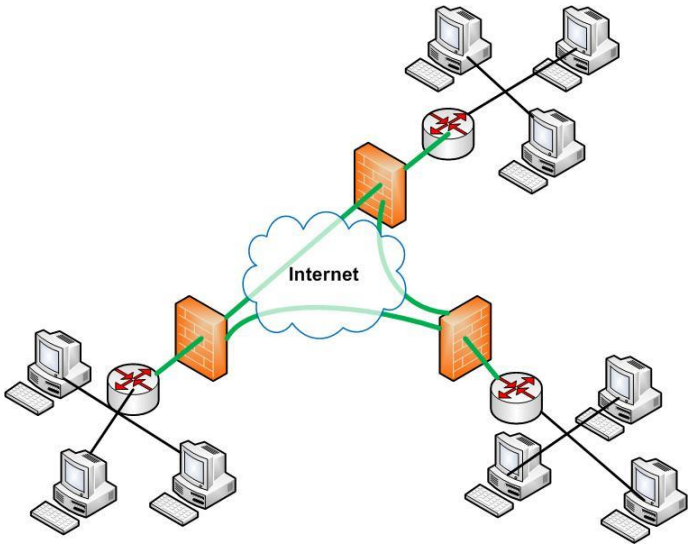
Salaus on todella merkittävässä roolissa tietoverkkojen tietoturvassa. Vahva salaus on Internetin tietoturvan peruste, siihen pohjautuvat tunnetuimmat metodit ovat

VPN:t, eli suomeksi näennäiset yksityisverkot ts. virtuaaliset erillisverkot, sekä TLS- (Transport Layer Security) protokolla, joka on SSL- (Secure Sockets Layer) protokollan kehittyneempi versio. Salausalgoritmeja voi olla joko symmetrisiä tai epäsymmetrisiä. Symmetrinen salaus sopii tietojen salaamiseen, kun taas todentamisessa ja allekirjoituksissa käytetään epäsymmetrisiä avaimia. Symmetrisissä salauksissa käytetään samaa avainta sekä salaamiseen että salauksen purkuun, siksi avaimen pitää olla ehdottomasti turvassa. Avainten vaihtoon sopii käyttää epäsymmetristä ts. julkisen avaimen salausta, koska silloin verkon yli voidaan turvallisesti lähettää salausavain, jota tarvitaan datan luottamuksellisuuden varmistamiseen. Tunnetuimpia symmetrisiä salausmenetelmiä ovat: AES (Advanced Encryption Standard), DES (Data Encryption Standard), 3DES (Triple Data Encryption Algorithm) ja Blowfish. Tunnetuimpia epäsymmetrisiä salausmenetelmiä ovat mm. RSA (Rivest-Shamir-Adleman cryptosystem) ja Diffie-Hellman algoritmi, näiden lisäksi myös TLS-protokolla käyttää salauksessa epäsymmetristä salausta. Digitaalisessa allekirjoituksessa käytetään myös sitä (DSA, Digital Signature Algorithm). [18]

3.2.2 Virtuaaliset erillisverkot

Virtuaalisia erillisverkkoja (VPN) tarvitaan silloin, kun kaksi fyysisesti erillään olevaa lähiverkkoa halutaan yhdistää turvallisesti julkisen verkon, ts. Internetin kautta. Turvallisuudella tarkoitetaan siirrettävän datan muuttumattomuutta sekä käyttäjän tunnistamista. Tunnistaminen ei kuitenkaan välttämättä tarkoita käyttäjien tunnistamista, vaan voi tarkoittaa verkkoyhteyden luomisessa osallistuvien laitteiden todentamista. Pitää muistaa myös, että VPN-tunnelia muodostaessa tarvitaan palomuurin yhteyttä molemmissa päässä. Kuten seuraavassa kuvassa nähdään, on erityisen tärkeää, että tunnelien salaus tehdään palomuurin sisäpuolella (Kuva 12). Kuvan esittämä periaate toteutuu myös silloin, kun kahdella verkkokortilla varustetussa palvelinlaitteessa pyörii sekä palomuuri että VPN-tunneliohjelmisto. IPsec on tunnetusti vahva tunnelointiprotokolla, joka toimii OSI-mallin (Open Systems Interconnection model) IP-kerroksella ja tukee myös IPv6-protokollaa. Se on riippumaton sovelluksesta, siis toimii laitteiden välillä, eikä vaikuta millään lailla käytettyihin sovelluksiin. [18]

OpenVPN-ohjelmisto on avoimeen lähdekoodiin perustuva SSL/TLS VPN-ratkaisu, joka käyttää UDP- (User Datagram Protocol) tunnelissa autentikointiin SSL/TLS- ja siirtoyhteyksissä IPSec (IP Security Architecture) ESP- (Encapsulating Security Payload) protokollaa. [23]

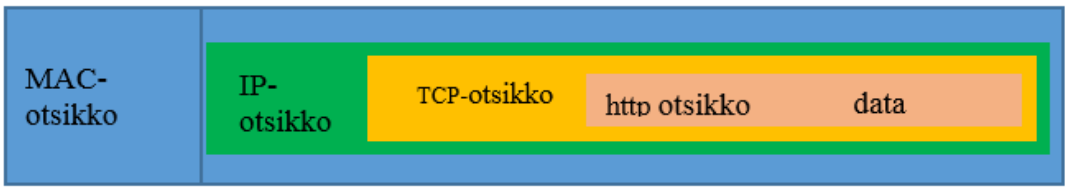


Kuva 12. Salaus alkaa VPN-tunnelien palomuurien sisällä

3.2.3 openVPN IP-tunnelin rakenne

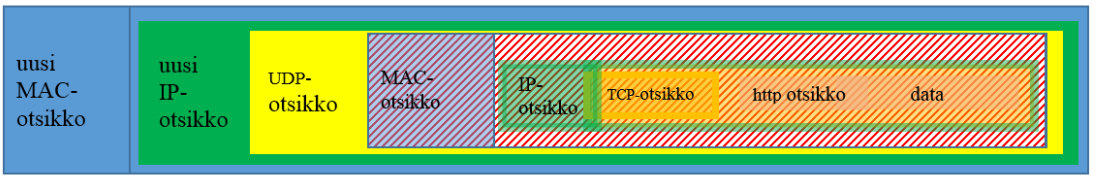
Tiedonsiirron tunnelointitekniikka perustuu TCP/IP- (Transmission Control Protocol) verkkojen paketointi-purku (engl. encapsulation-decapsulation) menetelmään, jonka ansiosta hyötykuorma (engl. payload), eli tieto ts. data voidaan kuljettaa paikasta toiseen käyttämällä erilaisia tapoja ts. protokollaa. OpenVPN on tunnetusti helppokäyttöinen, mutta kuitenkin vahvan salauksen omaava metodi. Tässä työssäkin on käytetty ns. staattisen avaimen salausmenetelmää, joka mahdollistaa että siirtokanava saadaan tietoturvallisesti käyttöön. Ennen tunnelin käynnistymistä pitää generoida ja jakaa salauksessa tarvittava yksityinen avain, sekä VPN-palvelimella että sen asiakaskoneella. Symmetrisen salauksen avain on 256-bittinen AES (Advanced Encryption Standard) ja VPN-istunnon kättelyssä todentaminen tapahtuu 160-bittisen SHA1- (Secure Hash Algorithm 1) tiivistearvon (engl. hash value) avulla. Tavallisesti Ethernet-kehys sisältää kaikki siihen paketoidun datan salaamattomana, se voidaan havaita OSI-mallia yksinkertaisemman TCP/IP-mallin avulla. Se on jaettu neljään

kerrokseen alhaalta ylöspäin, siirto- ja fyysinen-, verkko- (IP), kuljetus- (TCP/UDP), sovelluskerros. Esimerkkinä on kuva Internet-selaimen palvelupyynnön kehysrakenteesta (Kuva 13).



Kuva 13. Internet-palvelupyynnön Ethernet-kehys

Tunneloinnissa, jossa kaksi fyysisesti erillään olevaa verkkoa yhdistetään, tunnelin läpi pitää kuljettaa kokonaisia Ethernet-kehyksiä niin, että hyötykuorma, joka sisältää lähiverkon IP-otsikon, kuljetus-segmentin sekä sovelluskerroksen, salataan. VPN-palvelin suorittaa salauksen ja kehystää uudelleen niitä Ethernet-kehyksiä, joita on tarve kuljettaa tunnelin läpi. Tunnelin toisessa päässä, toinen VPN-palvelin purkaa tunnelista saapuvan Ethernet-kehyksestä salatun kuorman. Toisin, kuin salaamattomassa tiedonsiirrossa, VPN-tunnelin salattu kehysrakenne on kuvan mukainen (Kuva 14), jossa UDP-segmentin punaisilla raidoilla merkattu kuorma on salattu. OpenVPN-tunnelointimenetelmä vaihtaa kehyksen MAC- (Media Access Control address) osoitteen, IP-osoitteen. Kuljetusprotokolla on UDP, ja kehyksen salattu sisältö paljastuu vain tunnelin toisessa päässä. [13]



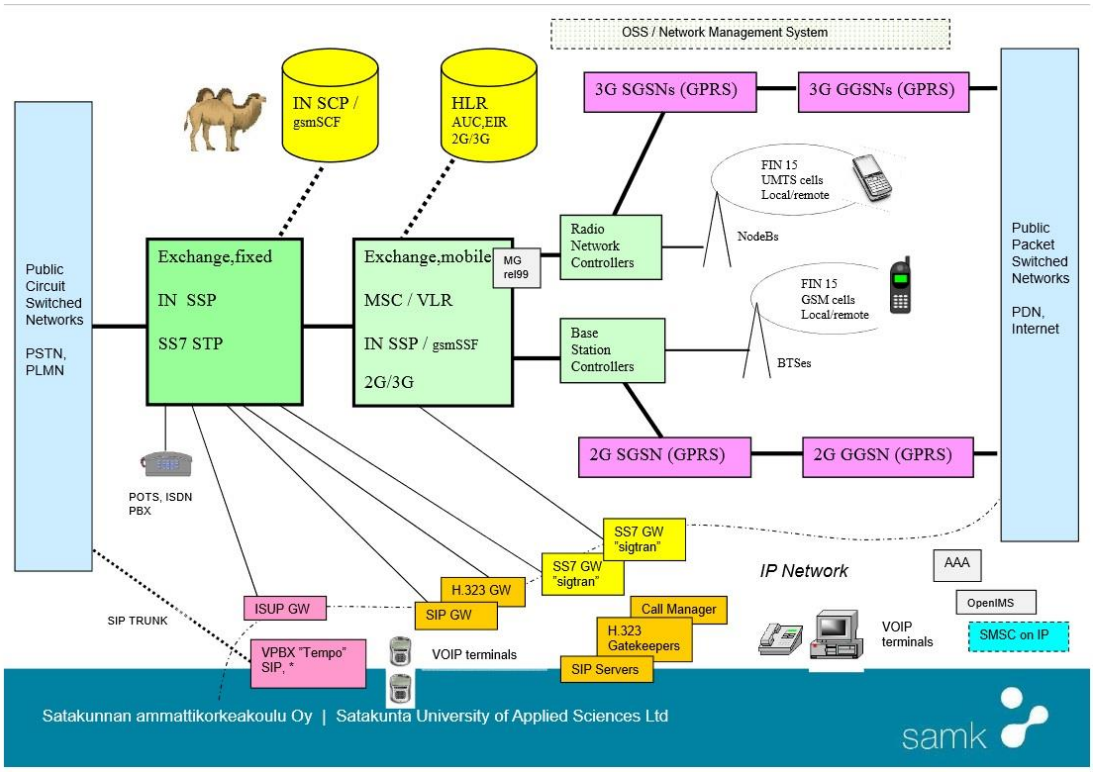
Kuva 14. Salattu kehysrakenne VPN-tunnelissa

4 ASENNUS

SAMK tarvitsee opetuksensa markkinointia varten liikuteltavan tukiaseman. Matkapuhelintekniikan esittäminen tuleville opiskelijoille sekä muille asiasta kiinnostuneille on haasteellinen tehtävä. Toimivan oman 3G-verkon esittäminen paikan päällä voi vaikuttaa paljon enemmän, kuin pelkkä luento hienon diaesityksen kera. GSM-puhelimia ja muita 3G-päätelaitteita voidaan liikuteltavan WBTS-tukiaseman avulla esittää käytössä sekä puhelimena että datapalvelujen asiakkaana, mm. Internetpalvelujen käyttäjänä. Kolmannen sukupolven verkkojen projektityöryhmän (3GPP) julkaisuissa tukiasemaa kutsutaan nimellä Node B, vaikka paljon yleisempiä nimityksiä niille ovat WBTS, BTS tai jopa pelkkä BS. [4] Työssäni käytän myös NSN laitteistonimeä Flexi WBTS, jonka nimi korostaa sen joustavuutta (engl. flexibility) asennuksissa.

4.1 NGN-laboratorion matkapuhelinkeskuksen laitteisto

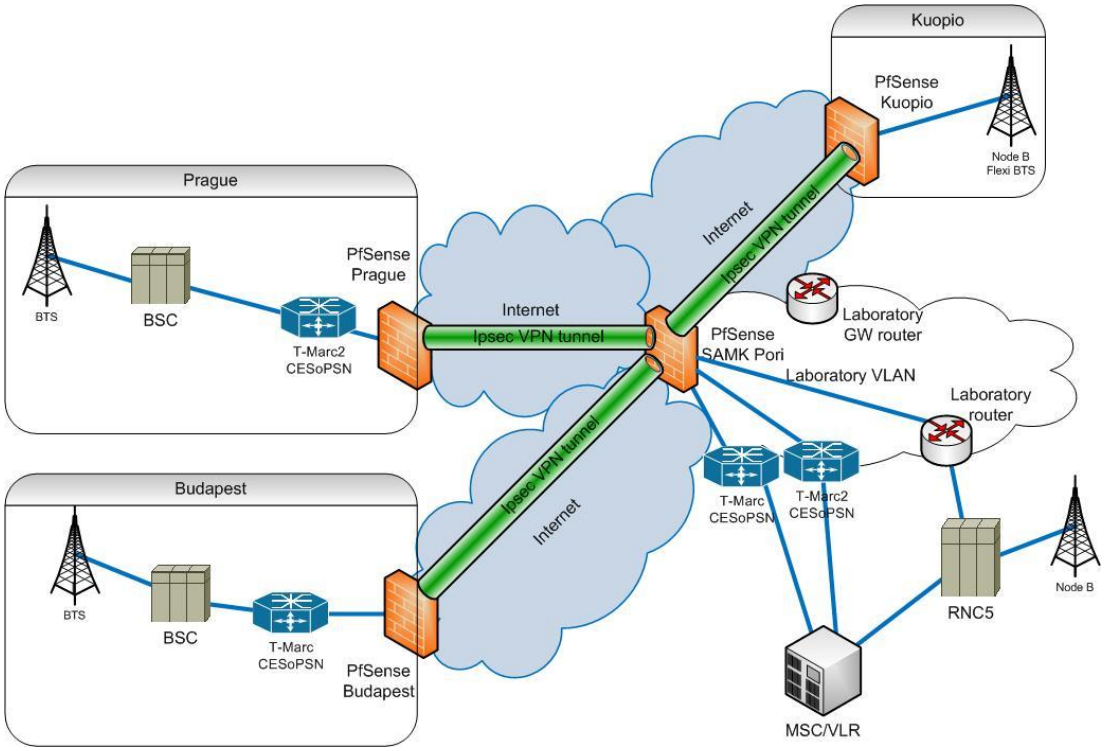
Matkapuhelinverkkojen opetuksessa opiskelijoiden käytössä on maailmanlaajuisesti ainutlaatuinen NGN-laboratorio. Kuva 15 esittää verkon topologian.



Kuva 15. SAMKin NGN-laboratorion laitteisto [1]

Opetuskäyttöön rakennettu puhelinkeskusjärjestelmä sisältää digitaalisen lankapuhelinkeskuksen lisäksi GSM-matkapuhelinjärjestelmän, mukaan lukien oman verkkotunnuksen: FIN 15. Puhelimet toimivat siis SAMKin omilla SIM-korteilla. Puhelinnumerot ovat osa globaalia puhelinnumerojärjestelmää ja niihin voi soittaa mistä tahansa maailmaa, mutta ilmeisesti kustannussyistä laboratoriosta ei voi soittaa ulospäin operaattoriverkkoon.

Laboratorion laitteistokanta päivittyy jatkuvasti niin, että eri valmistajien uudet koneet korvaavat vanhentuneen laitteiston, tai uuden palvelun vaativa laite kytketään järjestelmään. Tällä hetkellä (kesällä 2015) kolmannen sukupolven verkkotekniikan (3G) uusimpia laitteita edustavat 3GPP UMTS-spesifikaation Release 5-6:n mukaiset tekniikat. Matkapuhelinlaboratoriossa toimii sekä toinen (2G) että kolmannen sukupolven (3G) tukiasemia, koska samalla tavalla kuin kaupallisissa operaattoriverkoissa, myös opetusympäristössä siirtyminen uusiin tekniikkoihin tapahtuu vaiheittain. Paikallisten tukiasemien lisäksi puhelinkeskukseen on kytketty useita etätukiasemia viime vuosien aikana (Kuva 16).



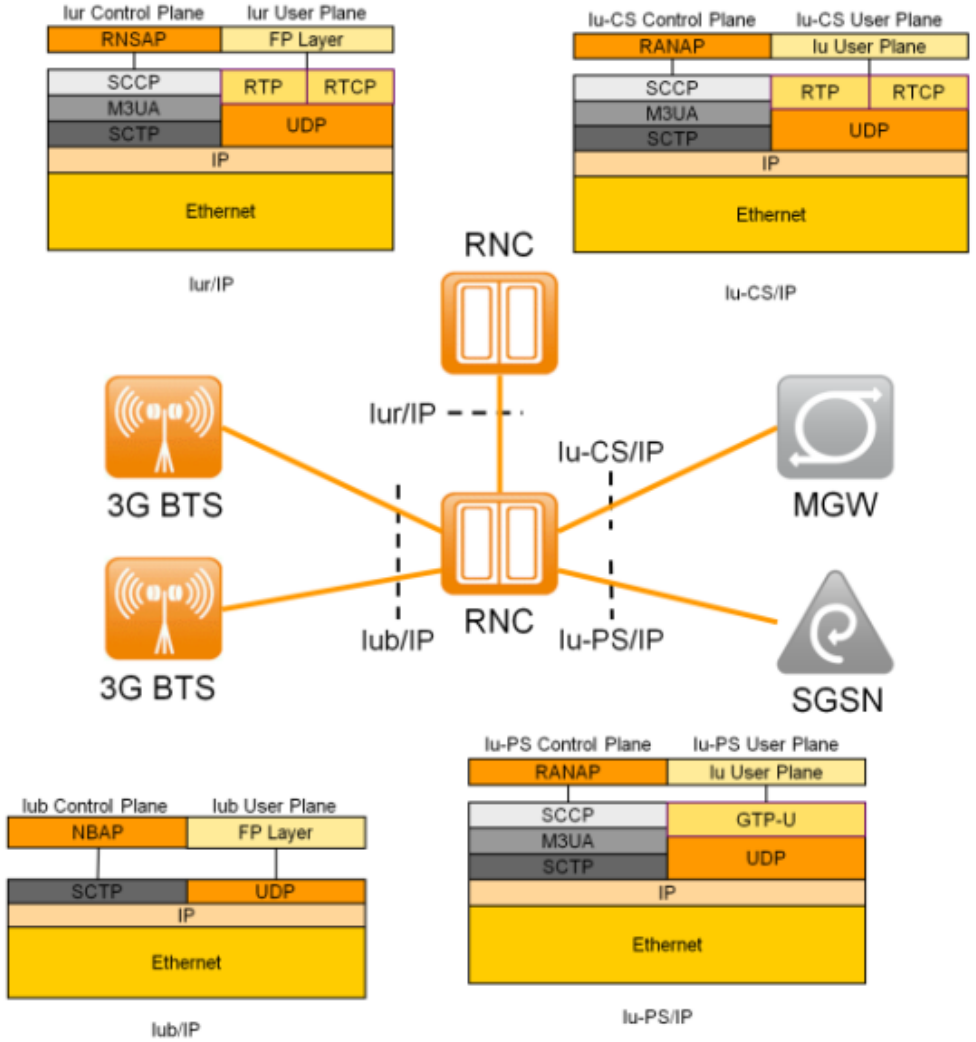
Kuva 16. Etätukiasemien tunneliyhteydet

Nykyään on kolme paikkaa, Budapest, Praha ja Kuopio, joista saadaan yhteyttä Poriin, kustannustehokkaasti IPsec VPN-tunnelien avulla Internetin kautta. Tunneleiden

toteutuksessa on käytetty avoimeen lähdekoodiin perustuvalla pfSense-ohjelmistolla asennettuja palvelimia, jotka on kytketty omien julkisten IP-osoitteiden kautta Internetiin. Päästä-päähän (engl. site-to-site) tapainen tunnelointi vaatii joko julkisen IP-osoitteen tai porttien uudelleenohjauksen (engl. port forward) tunneleiden päässä.

4.1.1 RNC radioverkko-ohjaimen tukiasemat

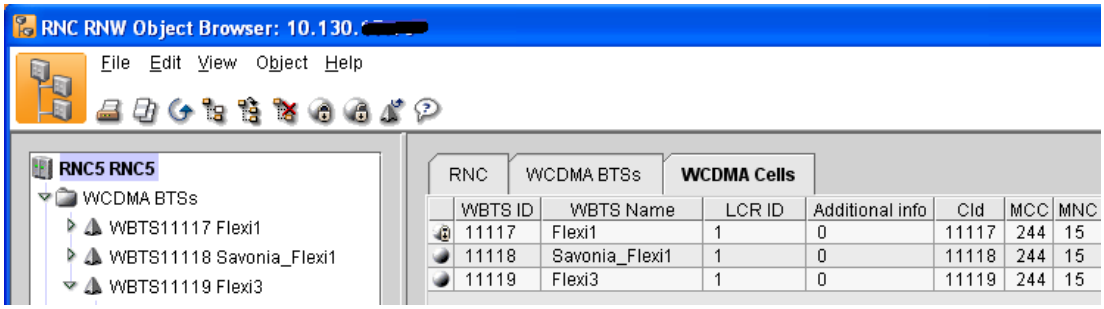
NSN RNC radioverkko-ohjain on matkapuhelinkeskuksen uusimpia laitteita. Seuraavan kuvan Iu-rajapintojen protokollapinoista nähdään, että RNC radioverkko-ohjaimen kaikki liitännät ovat IP/Ethernet-liittymiä (Kuva 17).



Kuva 17. RNC Iu-rajapintojen protokollat (Nokian opetusmateriaalia)

Ohjaimeen on kytketty parhaillaan kolme NSN Flexi WBTS-tukiasemaa, joista yksi on Kuopiossa Savonia ammattikorkeakoulun tiloissa. Kytketyt tukiasemat ovat:

WBTS 11117 Flexi1, WBTS 11118 Savonia_Flexi1, WBTS 11119 Flexi3. NSN:n Application Launcher/RNC RNW Object Browser on oivallinen työkalu radioverkko-ohjaimen tarkasteluun ja konfigurointiin. Sen avulla on todella kätevä ylläpitää matkapuhelinkeskuksen laitteita tietokoneelta verkon yli (Kuva 18).



Kuva 18. RNC radioverkko-ohjaimen tukiasemat.

Savonian tukiaseman Iub/IP-yhteys on toteutettu pfSense-palvelimen IPsec VPN-tunnelin kautta, muut tukiasemat on kytketty Ethernet-kaapelilla.

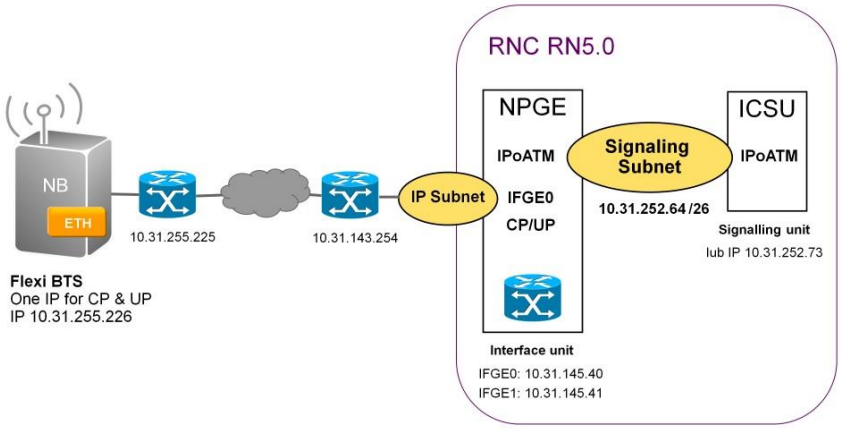
4.2 NSN Flexi WBTS-tukiaseman siirrettävyyden toteuttaminen

Tarkoitus on muuttaa Flexi3-tukiasema liikuteltavaksi. IP-yhteyden vaatimuksien tuntemus on tukiaseman onnistunut kytkennän edellytys.

4.2.1 WBTS tukiaseman IP-kytkentä

Itse tukiaseman asentaminen ei ole varsinaisesti osa tätä opinnäytetyötä, kuitenkin IP-yhteyksien määrittely onnistuu vain silloin, kun tiedetään miten tukiaseman signalointia ja dataliikennettä tapahtuu. Matkapuhelinlaboratorion UMTS-radiojärjestelmä (RAN, Radio Access Network) on toteutettu NSN:n laitteistolla, joka tukee UMTS Release 5 määrittelyn mukaista kytkentää. Valitettavasti laitteiston asennusohjeita ei ollut käytettävissä, mutta kaikki tarvittavat asiat selvisivät suhteellisen tarkasti Nokian WBTS-opetusmateriaalista. Toimivuuden edellytys on, että reitityksen on oltava kunnossa radioverkko-ohjaimen (RNC) aliverkoista WBTS-tukiaseman aliverkkoihin kumpaankin suuntaan. Reitityksiä toteutetaan asettamalla sopivia IP-asetuksia sekä tukiaseman että radioverkko-ohjaimen konfiguroinnissa, sen lisäksi kaikkien siirtotien reititinten reititystaulut on päivitettävä aina, kun järjes-

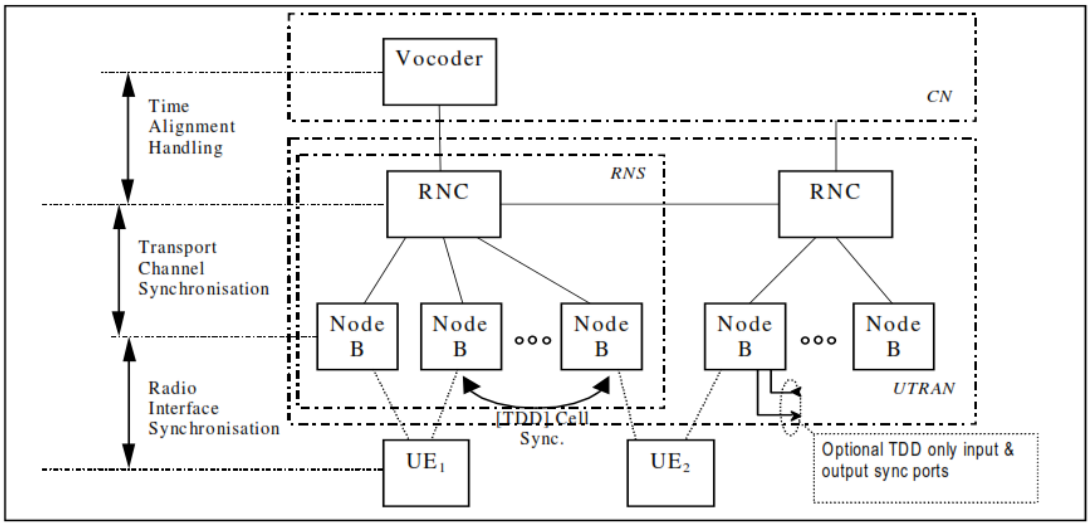
telmään asennetaan uusi tukiasema tai radioverkko-ohjain. Periaatekuva Iub/IP-kytkennästä on kuvassa (Kuva 19).



Kuva 19. WBTS-tukiaseman IP-yhteydet (Nokian opetusmateriaali)

4.2.2 Synkronointivaatimuksia

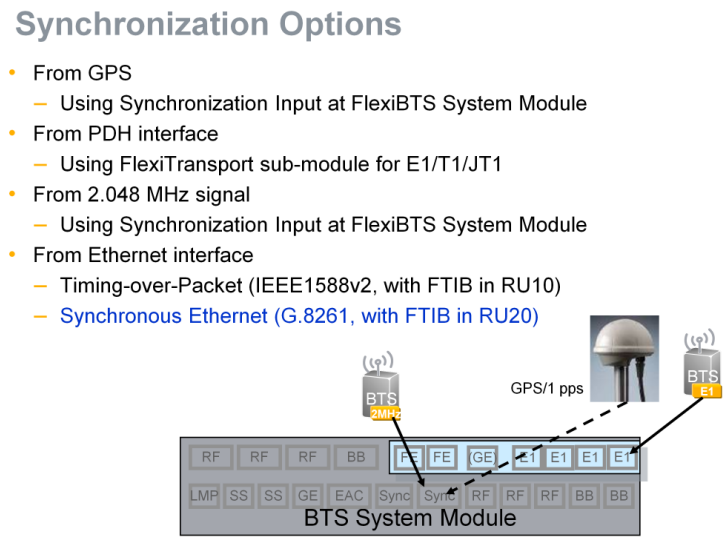
Standardien mukaan tukiasema kytketään järjestelmään niin, että se on synkronoitu runkoverkon kelloon. Eri rajapitojen synkronointivaatimukset on tarkkaan määritelty 3GPP:n spesifikaatioissa (Kuva 20). [3]



Kuva 20. UMTS-verkon synkronointi [3]

NSN Flexi BTS-laitteisto tarjoaa erilaisia mahdollisuuksia synkronointiin. Yksinkertaisin tapa on kytkeä aikajakomodulaatioon perustuvia E1/PCM- (Pulse-code Modulation) siirtolinkkejä, mikä takaa myös synkronoinnin. Erillinen synkronointi voisi olla GPS- (Global Positioning System) satelliitista tuleva signaali, joka vaatii lisälai-

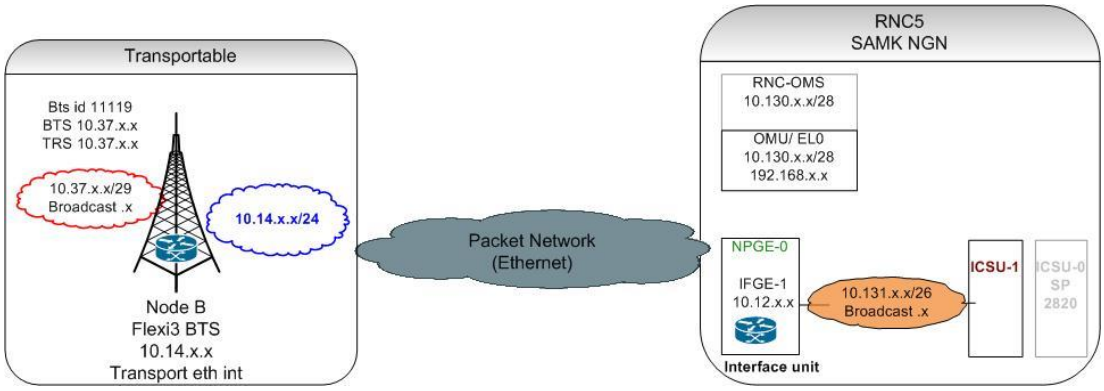
tetta tai toisesta laitteesta tulevan 2,048 MHz kellosignaalin, vaikkapa lähimmäisestä tukiasemasta. Ethernet-yhteyden kautta on tarjolla joko ToP- (Timing over Packet) menetelmä, joka käyttää PTP- (Precision Time Protocol) protokollan ajansiirtoa, tai ns. synkronoidun Ethernetin käyttöä (Kuva 21).



Kuva 21. NSN Flexi BTS synkronointia (Nokian opetusmateriaalia)

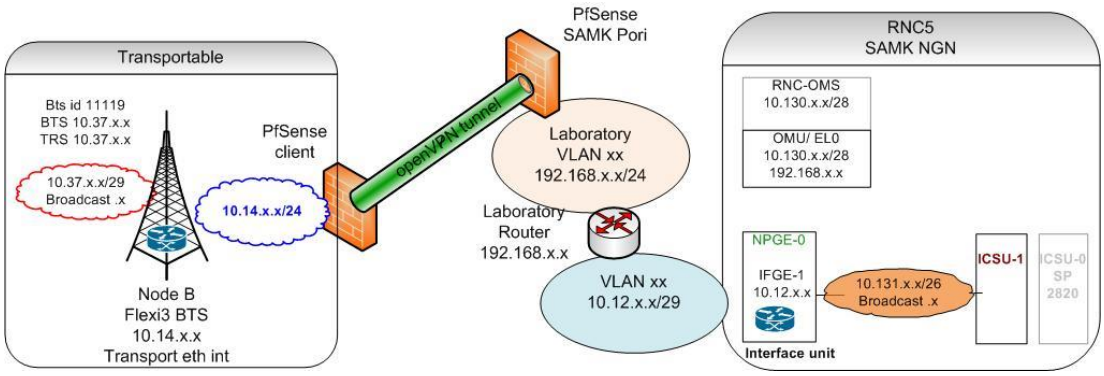
4.2.3 Flexi3 WBTS tukiaseman Iub/IP-rajapinta

Tukiasema on yhteydessä radioverkko-ohjaimeen SAMKin NGN-laboratoriossa pakettikytkentäisen IP-verkon, eli laboratorion lähiverkon kautta. Käytännössä ei ole merkittävää eroa, kulkevatko paketit Ethernet-verkkokaapelia pitkin, vai ohjataanko ne useiden verkkolaitteiden tai jopa Internetin kautta, jos ja kun paketit pääsevät perille (Kuva 22).



Kuva 22. Flexi3 tukiaseman ja RNC radioverkko-ohjaimen aliverkot

Matkapuhelinverkon pakettikytkentäisen yhteyden virittäminen on monimutkainen asia, jos kyseessä on laaja IP-verkko. Mikäli yhteys kulkee myös julkisen verkon kautta, tunnelointi on välttämätöntä, koska laitteiden välissä pitää olla saumaton yhteys. Reitityksen kannalta tunnelit toimivat niin, kuin saman reitittimen eri liitännät, eli niiden välissä on suora linkki. Edellisen takia pfSense palvelinten reititystaulua pitää päivittää asianmukaisesti niin, että reititys toimii moitteettomasti. Tukiaseman Iub-rajapinnan kytkentää IP-verkon kautta voidaan tarkastella seuraavasta kuvasta (Kuva 23).



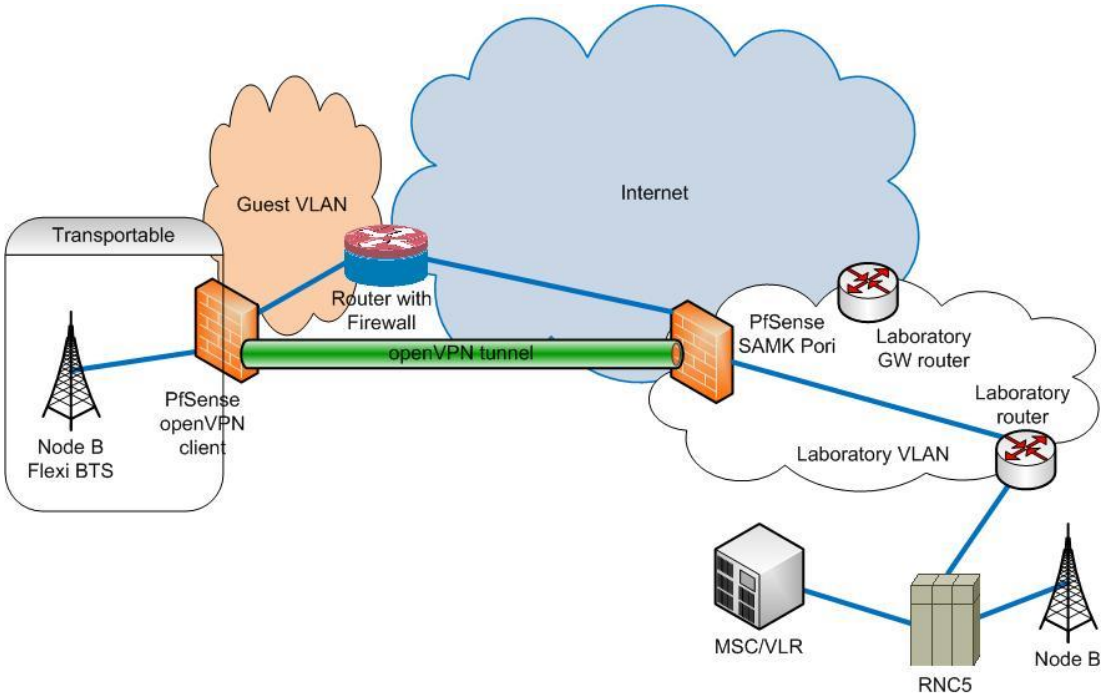
Kuva 23. Tukiaseman RNC-yhteyden aliverkot

Vaikka tunnelointi on rutiinitehtävä tietoliikennealan ammattilaiselle, tilapäistä käyttöä, esimerkiksi yhden päivän esittelyä varten, päästä-päähän tunnelin rakentamiseen kuluu kuitenkin liian paljon aikaa. Onneksi on muita mahdollisuuksiakin. Koska VPN-tunnelia on monta erilaista lajia, voidaan valita ns. asiakas-palvelinarkkitehtuuri, jonka toiminta etätietokoneelta vaatii ainoastaan pääsyn Internetiin ilman, että tarvitsisimme julkisen IP-osoitteen. Tähän tarkoitukseen sopii hyvin openVPN-tunneli ns. jaetulla avaimella, ilman mitään asiakastunnuksia ja salasanoja.

Tunneli rakennetaan käyttäen kahta tietokonetta ja asentamalla käyttöjärjestelmäksi FreeBSD Linux-jakeluun perustuvan PfSense 2.1-ohjelmiston. OpenVPN on suosittu avoimen lähdekoodin lisenssillä käytettävä tunnelointitekniikka, joka on tarjolla myös PfSense-ohjelmistossakin. Nimi: site-to-site, johtaa hieman harhaan, jos oletetaan, että kummatkin pfSense-koneet ovat kiinni Internetissä julkisilla IP-osoitteillaan. Kuitenkin yhteyden luonteesta johtuen, nimenomaan asiakaskone (engl. client) voi olla myös reitittimen takana lähiverkossa, koska yhteydenotto tunnelia varten lähtee aina asiakkaalta palvelimeen päin. Näin olleen, samalla tavalla kuin In-

ternet-sivuja selatessa, asiakaskone lähettää pyynnön yhteydenottoa varten VPN-palvelimeen ja tunneliyhteys luodaan heti, kun palvelin hyväksyy sen. Johtuen edellisestä, asiakaskoneen palomuuriin ei vaadita mitään pakollista sääntöä pakettien suodatukseen. [5]

PfSense-koneiden tarkat asennusohjeet perustuvat verkkojulkaisuun [2], jonka voi lukea liitteestä 2. Ensimmäisen konfiguroinnin jälkeen tunneli on valmis käyttöön heti, kun virta on kytketty tietokoneeseen, joka toimii tunneliarkkitehtuurin asiakkaana (Kuva 24).



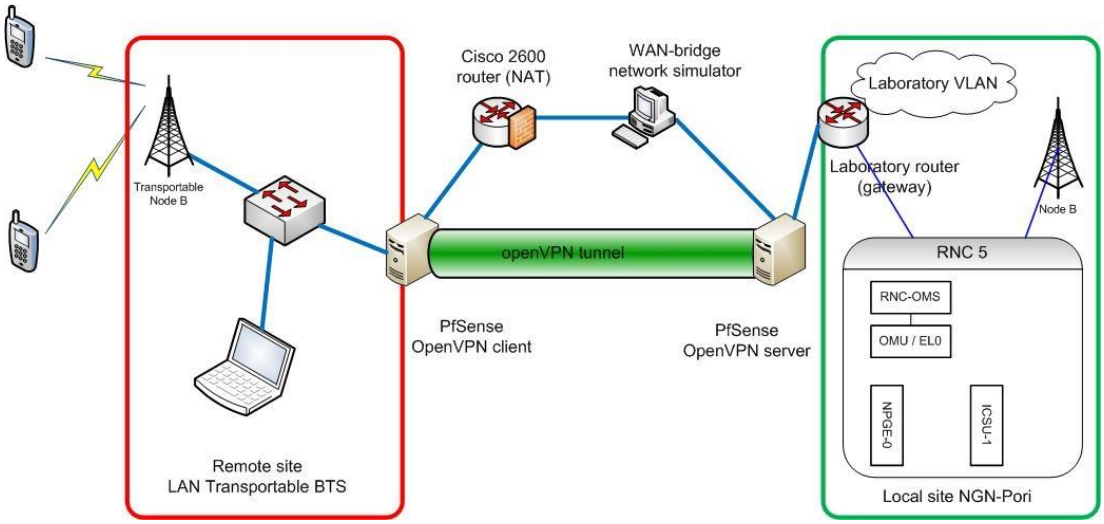
Kuva 24. Periaatekuva 3G-tukiaseman IP-yhteyden tunneloinnista

Sama pfSense-palvelin, joka hoitaa IPsec VPN-tunneleita Budapestiin, Savonia ammattikorkeakouluun Kuopioon ja Prahaan, pystyy hoitamaan myös openVPN-tunnelin siirrettävän tukiaseman suuntaan.

4.2.4 Flexi3 tukiaseman koekytkentä

Saadaksemme Flexi3 tukiaseman siirrettäväksi on kokeilua varten rakennettava testiympäristö, joka vastaa lopullista topologiaa, mutta ei kuitenkaan haittaa matkapuhelinlaboratorion toimintaa. PfSense asiakas-palvelinarkkitehtuuria varten on hankittu kaksi vanhaa pöytäkonetta tietohallinnosta, joihin on kumpaankin asennettu integ-

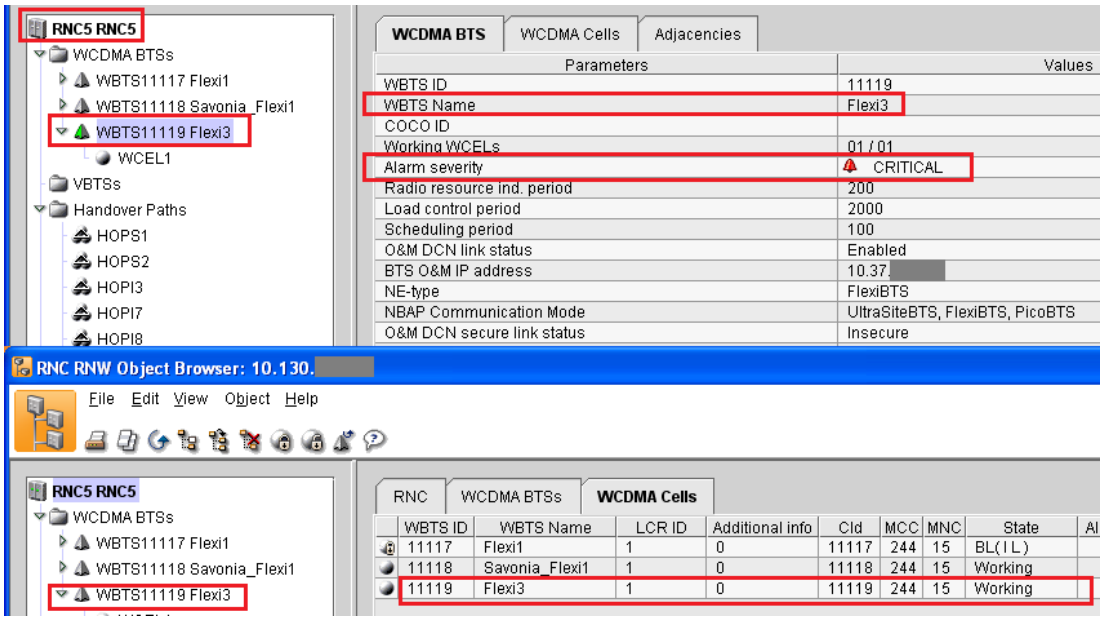
roidun verkkokortin lisäksi PCI- (Peripheral Component Interconnect) verkkokortti. Cisco 2600 reititin toimii ikään kuin palomuuri-reititinlaite erässä vieraille tarkoitetussa lähiverkossa, DHCP- (Dynamic Host Configuration Protocol) palvelimena se jakaa IP-osoitteita, muttei kuitenkaan ole kytketty Internetiin. Sen sijaan pfSense-palvelimeen on kytketty kiinni käyttämällä kiinteitä, periaatteessa julkisia, testikäyttöön keksittyjä IP-osoitteita. WAN-Bridge (WAN, Wide Area Network) verkkosimulaattori on kytketty vain testausten loppuvaiheessa. Laitteiden luetteloa voidaan tarkastella liitteestä 1, josta löytyy paitsi laitemerkki ja malli, myös niiden ohjelmistoversio. Liikuteltavaan ympäristöön kuuluu myös kuvassa kannettavaksi piirretty työasema, sen tarkoitus on testata pingaamalla verkon toimintaa, sekä avata matkapuhelinverkon työkaluilla yhteys puhelinverkon laitteisiin, kuten tukiasemaan, radioverkko-ohjaimeen ym. (Kuva 25).



Kuva 25. Testiympäristön topologia

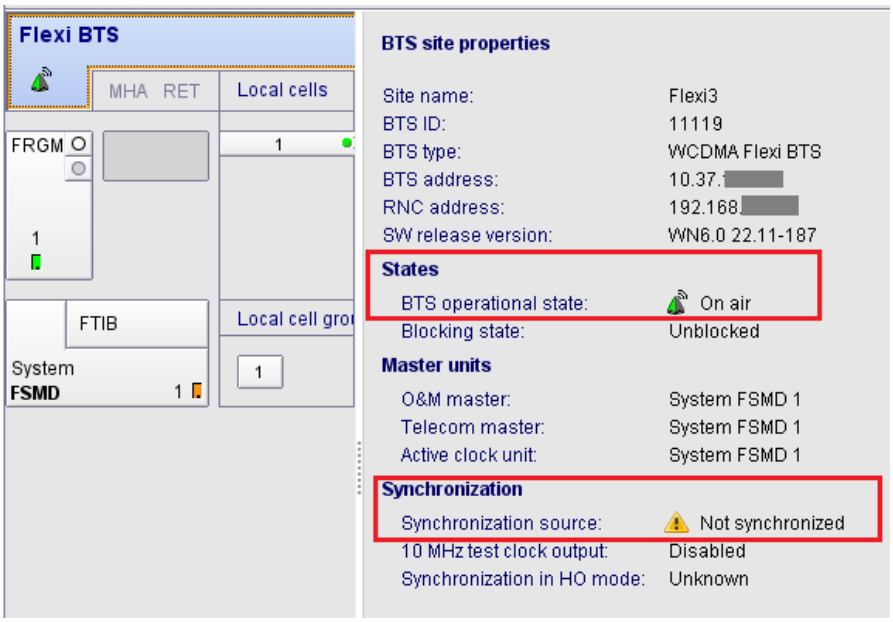
4.2.5 Tukiaseman ja RNC:n laitteistojen tilannekatsaus

NSN työkaluilla voidaan tarkastella laitteiston tilannetta. Tilannekatsaus on suoritettu silloin, kuin puheluyhteydet onnistuvat niiden kautta ongelmitta. Otetaan yhteyttä RNC radioverkko-ohjaimeen, tukiaseman lähiverkkoon kytketystä tietokoneelta (Kuva 26).



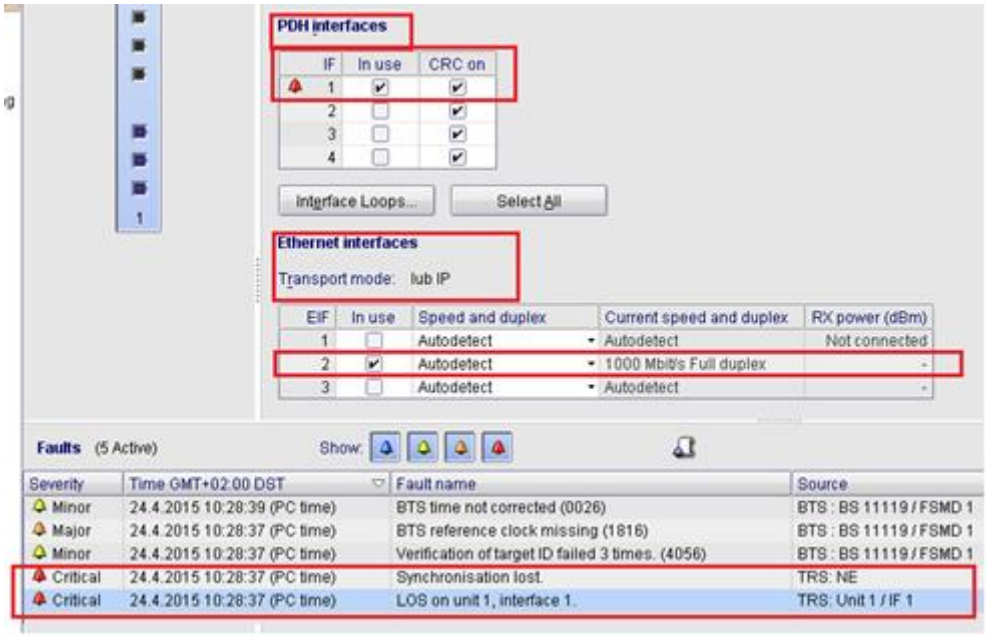
Kuva 26. RNC:een kytketty siirrettävä tukiasema WBTS 11119 Flexi3

Tukiasema on toiminnassa, mutta kriittinen hälytys on ilmestynyt. Voidaan tarkastella myös tukiaseman tilannetta, josta saadaan tietoa hälytyksen syystä (Kuva 27).



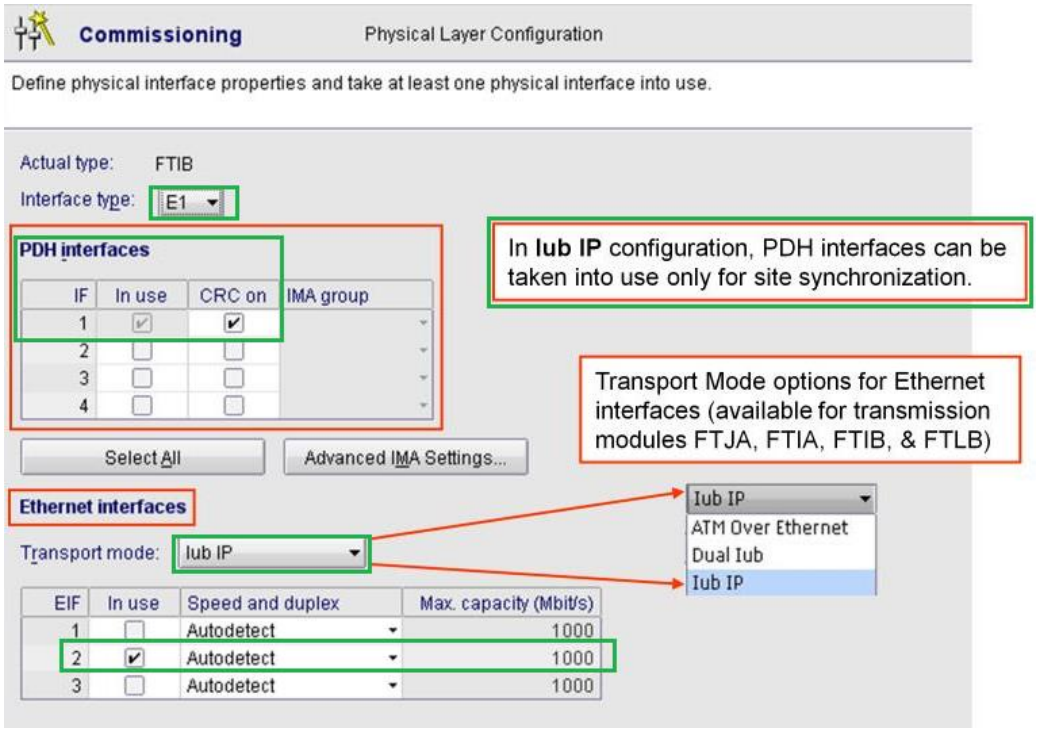
Kuva 27. Flexi3 tukiaseman tilanne

Hälytyksen aiheuttaja on synkronoinnin puute, sen takia koska PDH- (Plesiochronous digital hierarchy) liittymä on merkattu käytössä olevaksi, mutta ei ole kuitenkaan kytketty. Laite olettaa saavansa kellosignaalin E1/PCM liittymän aikavälistä. Käytännössä ei ole havaittu mitään virheitä, vaikka synkronointi, vastoin laitteiston ohjeen vaatimuksia, tosiaan on ratkeamatta. Hälytyksen aiheuttaja on seuraavan kuvan mukaisesti käytössä olevan PDH-liitäntä (Kuva 28).



Kuva 28. Flexi3 tukiaseman PDH-liitäntä aiheuttaa hälytyksen

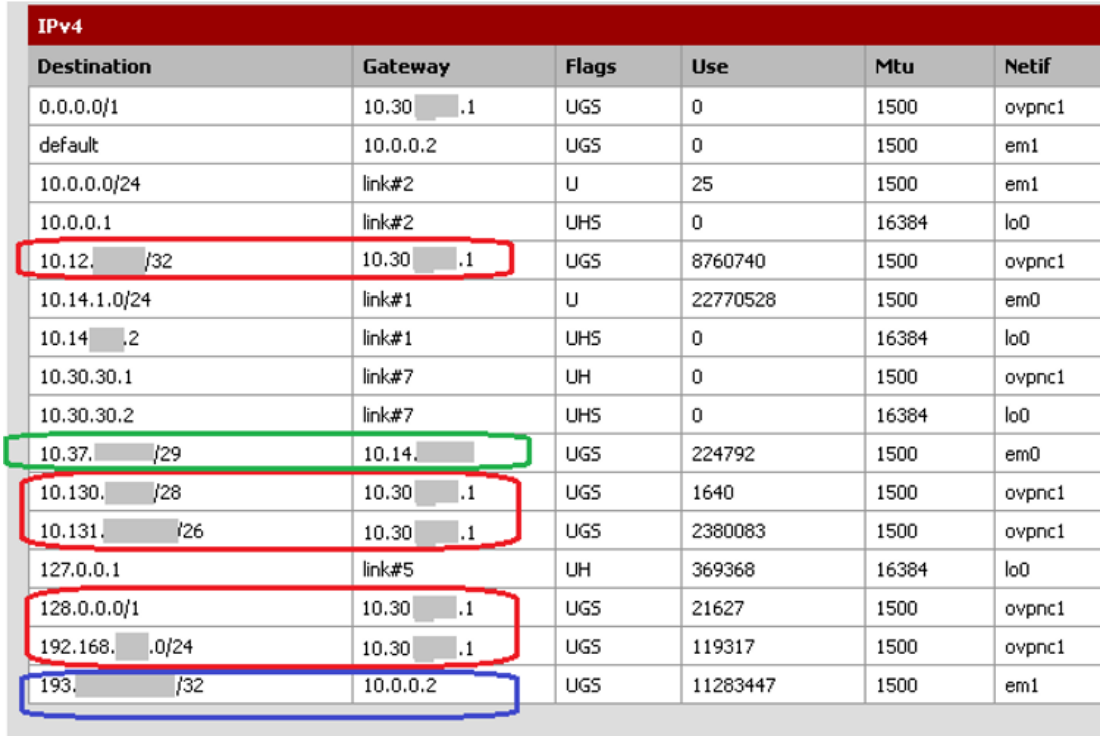
Myös NSN:n opetusmateriaalin mukaisesti PDH-liittymä voidaan kytkeä vain synkronointikäyttöön, silloin kun siirtoyhteys on IP:n mukainen Iub-rajapinnan kautta (Kuva 29).



Kuva 29. PDH liittymän käyttö vain synkronointia varten. (Nokian opetusmateriaalista)

4.2.6 Reitityksiä tunnelin kautta

On syytä tarkastella, mitkä reitit ovat kulkueessa tunnelin läpi, yhteydessä tukiasemasta radioverkko-ohjaimeen (Kuva 30 ja Taulukko 1).



IPv4

Destination	Gateway	Flags	Use	Mtu	Netif
0.0.0.0/1	10.30 .1	UGS	0	1500	ovpnc1
default	10.0.0.2	UGS	0	1500	em1
10.0.0.0/24	link#2	U	25	1500	em1
10.0.0.1	link#2	UHS	0	16384	lo0
10.12. /32	10.30 .1	UGS	8760740	1500	ovpnc1
10.14.1.0/24	link#1	U	22770528	1500	em0
10.14 .2	link#1	UHS	0	16384	lo0
10.30.30.1	link#7	UH	0	1500	ovpnc1
10.30.30.2	link#7	UHS	0	16384	lo0
10.37. /29	10.14.	UGS	224792	1500	em0
10.130. /28	10.30 .1	UGS	1640	1500	ovpnc1
10.131. /26	10.30 .1	UGS	2380083	1500	ovpnc1
127.0.0.1	link#5	UH	369368	16384	lo0
128.0.0.0/1	10.30 .1	UGS	21627	1500	ovpnc1
192.168. .0/24	10.30 .1	UGS	119317	1500	ovpnc1
193. /32	10.0.0.2	UGS	11283447	1500	em1

Kuva 30. Reititystaulukko pfSense-client koneelta.

Taulukko 1. PfSense-client koneen reititystaulukko tukiaseman reittiä varten

kohteen IP-osoite	**yhdyskäytävä**	**selitys**
oletusreitti (default)	10.0.0.2	Cisco reititin koekytkennässä Vieraassa verkossa yhdyskäytävä nettiin
10.12.x.x	10.30.x.1	RNC:n IP-aliverkkoon openVPN-tunnelin kautta
10.37.x.x/29	10.14.x.1	Flexi3 tukiaseman BTS/TRS-aliverkkoon tukiaseman ethernet liittymän kautta
10.130.x.x/28 10.131.x.x/26	10.30.x.1 10.30.x.1	RNC:n OMS/OMU:n ja ICSU:n signaloinnti, openVPN-tunnelin kautta
192.168.x.0/24	10.30.x.1	Laboratorion verkko, openVPN-tunnelin kautta
193.x.x.x/32	10.0.0.2	pfSense-serveriin Internetin kautta

Edellinen kuva ja taulukko esittävät pfSense-client koneen reititystaulukkoa, tunnelin läpi kulkevat punaisella merkityt reitit. Taulukosta selviävät myös reittien tarkoitukset.

4.3 Testaus

Tavallisesti verkkoyhteys paikallisen tukiaseman ja RNC:n välillä on suora kuparitai kuitulinkki. Sen sijaan etätukiaseman verkkoyhteys on VPN-tunneli, joka kulkee usean verkkolaitteen kautta ja tästä johtuen tiedonsiirrossa esiintyy sekä viivettä että pakettien katoamista. Testauksessa simuloidaan pitkien yhteyksien aiheuttamia häiriöitä tietokoneeseen asennetulla WAN-Bridge nimisellä sovelluksella, joka toimii OSI-mallin siirtokerroksessa puuttumatta pakettien IP-osoitteisiin.

4.3.1 Verkkoemulaattori

Kahdella verkkokortilla varustettu tietokone on helppo työkalu myös pitkien verkkoyhteyksien jäljittämiseen. Käynnistämällä USB-muistilta WAN-Bridge nimisen sovelluksen saadaan aikaan verkkoemulaattori, jonka asetuksia muuttamalla verkkoyhteys muuttuu, ikään kuin oikeassa Internetyhteyksissä, hitaammaksi, jopa data paketteja häviää. Ohjelma toimii OSI-mallin siirtokerroksella, eli siihen ei tarvitse muuttaa mitään verkkoasetuksia, eikä se myöskään vaikuta pakettien reititykseen. Kirjoittamalla komentoriville: *wanbridge menu*, ohjelma tarjoaa vaihtoehtoisia asetuksia tai mukautetussa tilassa *custom*, käyttäjä voi itse muokata sekä viiveen, kaistaleveyden ja pakettihäviön asetuksia (Kuva 31).

```
WAN-Bridge Live-CD v1.10

Please select one of the following options:
-------------------------------------------
1: 40ms  round-trip delay, 1544Kbps, 0.1% packet loss
2: 60ms  round-trip delay, 1544Kbps, 0.1% packet loss
3: 80ms  round-trip delay, 1544Kbps, 0.1% packet loss
4: 100ms round-trip delay, 1544Kbps, 0.5% packet loss
5: 120ms round-trip delay, 1544Kbps, 0.5% packet loss
6: 120ms round-trip delay, 768Kbps , 0.5% packet loss

status:   Show Current settings
custom:   Custom WAN Settings
dhcp:     Get DHCP Address
static:   Set Static Address
ip:       Show IP Address
tz:       Set Time Zone
stop:     Stop WAN Emulation
q:        Exit

Selection? _
```

Kuva 31. WAN-Bridge sovelluksen komentorivivalikko. [6]

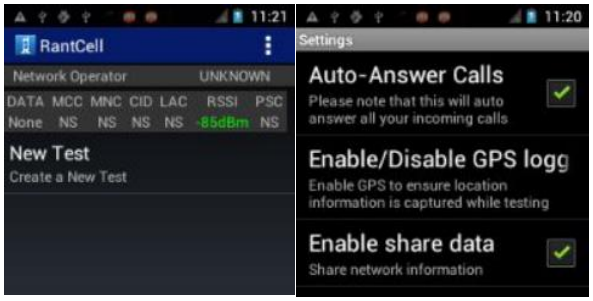
4.3.2 Testauksia käytännössä

Tukiaseman toimintaa kokeiltiin Nokia E71 kännykällä, joka rekisteröityy luotettavasti verkkoon. Varsinaiset testipuhelimet olivat Android-puhelimia. Ilmaisia, testaukseen ja verkon tarkasteluun sopivia sovelluksia on saatavissa runsaasti Google Play verkkokaupasta. Testisoitto on soitettu käyttämällä RantCell nimistä sovellusta. Matkapuhelinverkon tarkastelu suoritettiin G-NetTrack Lite ohjelmalla. Matkapuhelinten näyttökaappauksia otettiin kätevästi yhdistämällä puhelin tietokoneeseen Mobizen sovelluksella.

NGN-laboratoriossa toimii koko ajan myös GSM-verkon 2G-tukiasema. Sen kautta puhelimet pääsevät verkkoon, käyttämättä testin kohteena olevaa liikuteltavaa 3G-tukiasemaa (Flexi3). On varmistettava, että käytetyt puhelimet valitsevat aina UMTS-verkon. Nokian E71 puhelimesta valitaan: *>Menu >Tools >Settings >Phone >Network >Network mode> * UMTS*, joka tarkoitta ainoastaan 3G-verkkoa. Android laitteissa ei välttämättä menuvalikosta löytyy vastaava, mutta verkon pääsee valitsemaan soittamalla testinumeroon: **#*#4636#*#** ja määrittämällä sen: *>Testing >* Phone Information >Set preferred network type >*WCDMA only*.

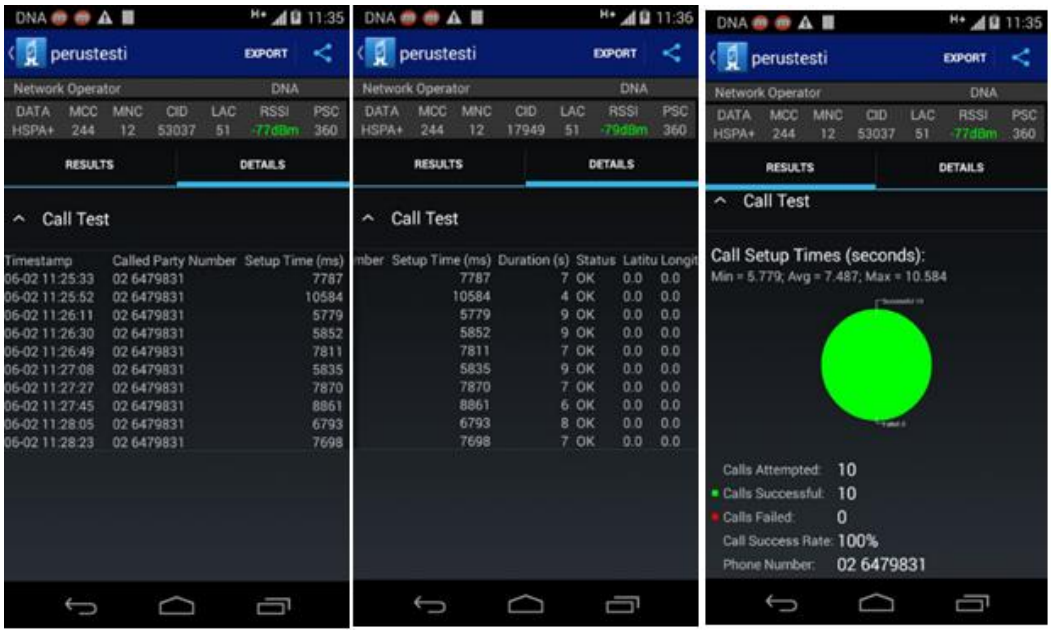
4.3.3 Testisoitto ulkoverkosta

SAMKin NGN-laboratorion puhelinkeskus on linkitetty Suomen puhelinverkkoon ja ottaa vastaan puheluita, kuitenkin SAMKin puhelimet voivat soittaa vain sisäisiä puheluita. Ensimmäinen testisoittosarja soitettiin dna-verkosta. Android kellossa, puhelinnumero: 02 647 9831, asetettiin automaattinen vastaus, testissä käytetyn sovelluksen kautta. *RantCell >settings >Auto-Answer Calls, enabled* (Kuva 32).



Kuva 32. Automaattisen vastauksen asettaminen

Puhelun vastaanoton testaus 10 kertaa RantCell sovelluksella. Soitettu yleisestä matkapuhelinverkosta (operaattori dna, MCC=244 MNC=12), onnistumisprosentti 100 % (Kuva 33). Koska testaustuloksiin on vaikuttanut oleellisesti radiokentän epävakaus selvittämättömästä syystä, testisoitto suoritettiin tukiaseman (WBTS) välittömästä läheisyydestä. Toimistohuoneessakin on ollut radiokenttä kiitettävällä tasolla, mutta soittoja on epäonnistunut useasti sieltä soitettuna.

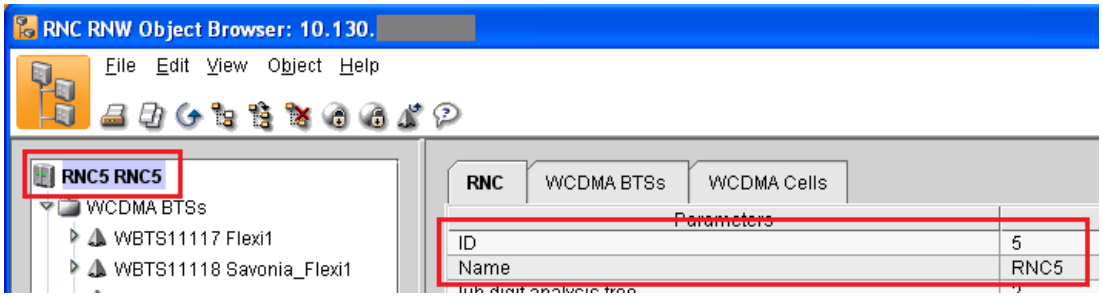


Kuva 33. Testisoittojen tilastotiedot

Matkapuhelinverkon tilanne nähdään puhelimesta G-NetTrack sovelluksella (Kuva 34). Sitä tutkimalla voidaan tarkastella yhteysasetuksia.

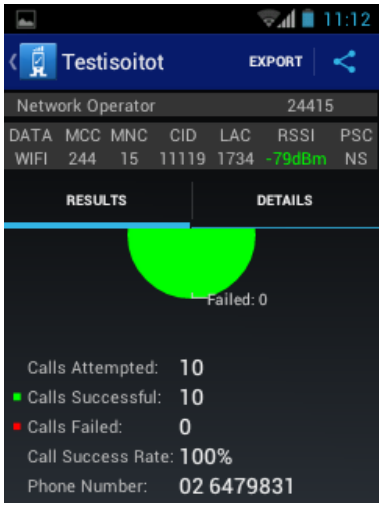
Kuva 34. Soittavan puhelimen verkko-ominaisuuksia

Verkko-operaattori on tunnistettava Suomen maakoodista MCC: 244 ja palvelutarjoajan tunnuksesta MNC: 15. Radiokentän voimakkuus RSCP: -81dBm on hyvällä tasolla. Radioverkko-ohjaimen tunnus on RNC:5, vastaa todellisuutta (Kuva 35). Tukiaseman tunnus CELLID: 11119 ja verkon tyyppi Type: UMTS ovat liikuteltavan Flexi3 tukiaseman arvoja.



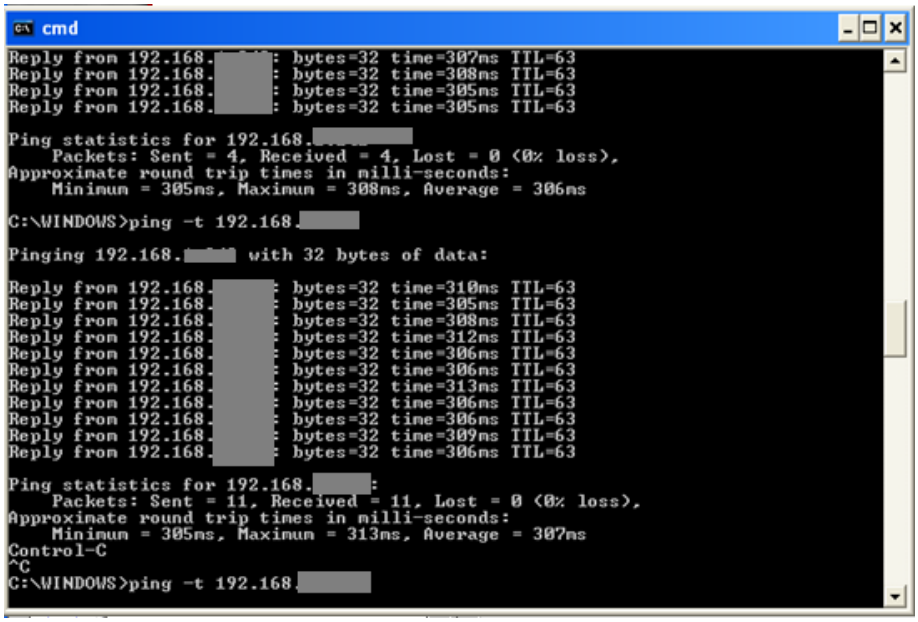
Kuva 35. Radioverkko-ohjaimen tunnus

Testisoitot kahden älypuhelimen välissä, kun molemmat ovat kiinni samassa Flexi3 tukiasemassa (BTS ID:11119). Kaikki soitot onnistuivat (Kuva 36).



Kuva 36. Onnistuneet soitot

Viiveen ja pakettien katoamisen vaikutuksia yhteyden laatuun on testattavissa WAN-Bridge ohjelman avulla. Sovelluksessa määritelty viive on edestakainen aikalisäys ja se näkyy ping-pakettien kulkuajoissa VPN-tunnelin läpi, kun on asetettu arvoksi 300 ms (Kuva 37). Pitkät etäisyydet tukiaseman ja RNC:n välissä vaikuttavat merkittävästi siihen, saadaanko VPN-tunnelin kautta yhteyttä tukiasemasta runkoverkkoon.



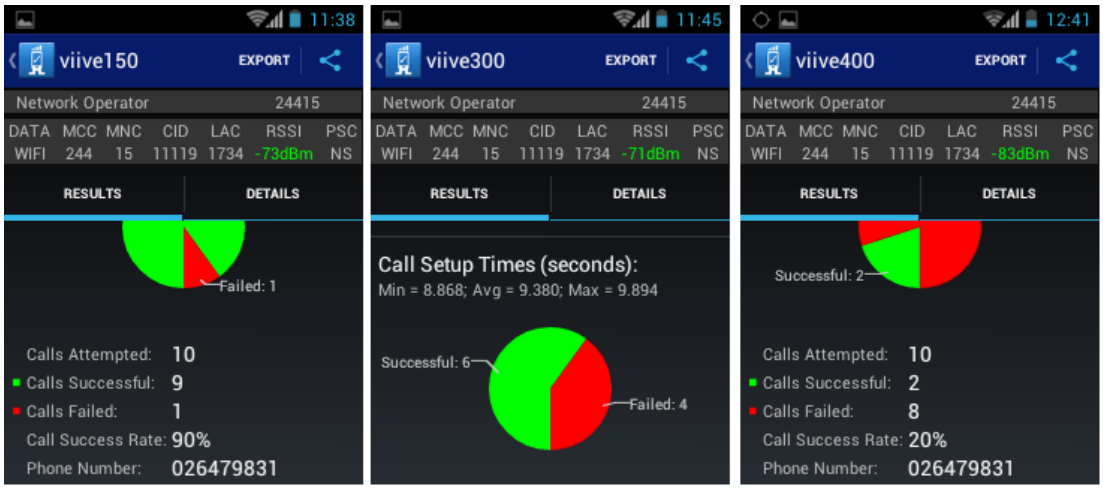
Kuva 37. Ping-testi työasemasta tukiaseman lähiverkosta (10.14.x.0) laboratorio-verkkoon (192.168.x.0) kautta openVPN-tunnelia

Testisoittojen yhteenveto on seuraavassa taulukossa (Taulukko 2). Niin kuin voi arvata, viiveet eivät vaikuta tiedonsiirtoon niin paljon, kuin pakettien häviäminen. Jopa 400 ms viiveellä yhteydet toimivat 80 prosenttisesti hyvin jos kaikki paketit pääsevät perille asti.

Taulukko 2. Testisoittojen yhteenveto

Kaistaleveys (Bandwith)[Kbps]	**Viive** (round-trip latency /delay) [ms]	**Hävikki** (PLR, packet loss rate) [%]	**Onnistumisprosentti** [%]
1544	150	0	100
1544	150	2	90
1544	300	0	90
1544	300	2	60
1544	400	0	80
1544	400	2	20

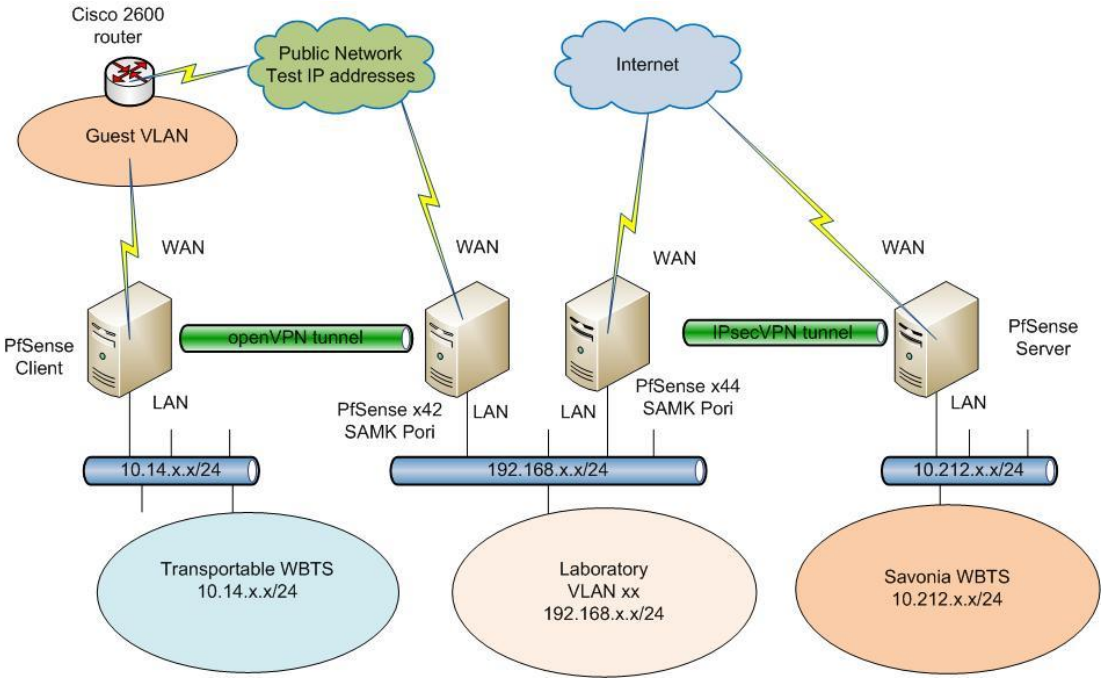
Pakettien hävikin vaikutus kasvaa, jos samalla viivekin suurenee, yhteyden laatu on epäluotettava, koska enää 20 % onnistuu (Kuva 38).



Kuva 38. Viiveen vaikutus kun pakettien hävikki on 2%

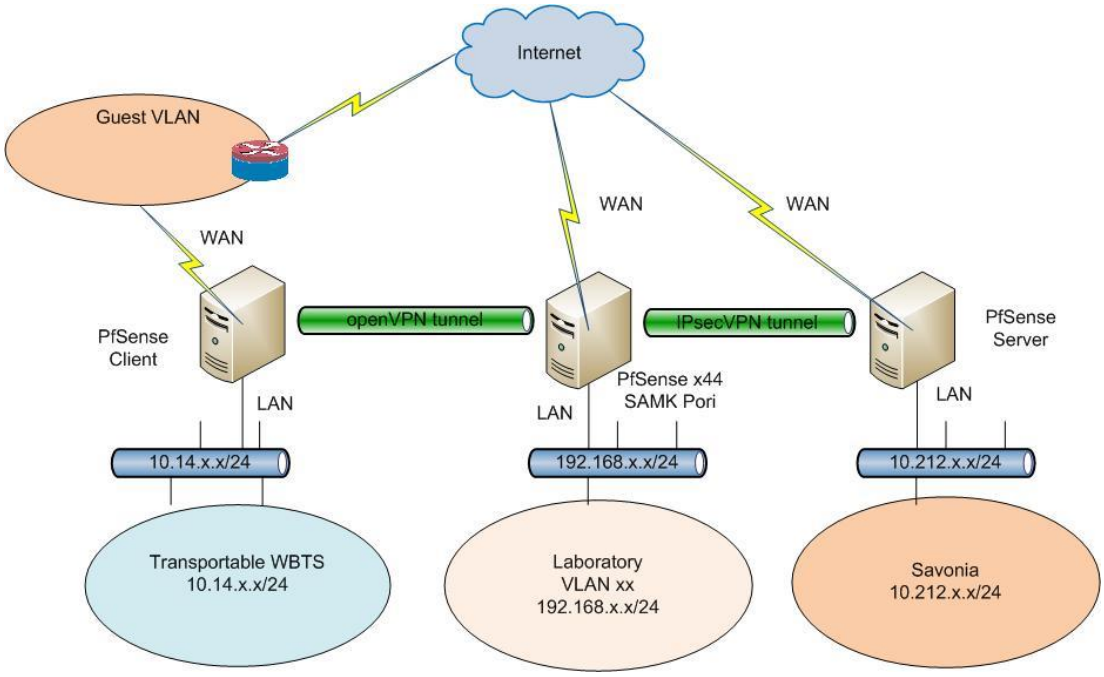
4.4 Tunneliyhteyden pysyvä asentaminen NGN-laboratoriossa

Koekytkennän onnistuttua openVPN-tunneli ja siihen tarvittavat reitit-ykset on siirrettävä matkapuhelinlaboratorion pysyvään kokoonpanoon. Tunnelitopologia testauksen aikana matkapuhelinkeskuksen lähiverkossa on ollut kuvan mukaista (Kuva 39).



Kuva 39. Matkapuhelinverkon tunnelit openVPN-testauksen aikana

Seuraavaksi pfSense-x42-palvelin irrotetaan verkosta, sen asetukset siirretään pfSense-x44-palvelimeen ja päivitetään laboratorioverkon reitittimien reititystaulukkoja uuden topologian mukaiseksi. Verkon kuva muuttuu näin (Kuva 40).



Kuva 40. Tunneleiden kytkennät pfSense-palvelimien välissä

5 YHTEENVETO

Aiheenvalintaan vaikutti, että viihdyn hyvin laiteasennusten parissa ja sain tehtäväksi haasteellisen asennus- ja tutkimustyön. SAMKin tietoliikenneopetuksen matkapuhelinlaboratorio tarvitsee liikuteltavan tukiaseman 3G-tekniikan esittelyä ja erilaisia projektia varten, joiden yhteistyökumppanit voivat olla eri paikoissa Suomessa tai jopa ympäri maailmaa.

Tein tutkimusta matkapuhelinverkkojen kehityksestä, etenkin 3G-verkoista. 3GPP:n Release 5 suosituksen myötä, NodeB:n ja RNC:n välinen linkki voi olla IP-pohjainen, mikä mahdollistaa myös, että tukiaseman tietoliikenne kulkee lähiverkossa (LAN, Local Area Network) tai Internetissä. Tutustuin perinpohjaisesti NGN-laboratorioon hiljattain asennetun radioverkko-ohjaimen (RNC) toimintaan ja sen yhteyteen VPN-tunnelin kautta Savonia AMK:ssa sijaitsevaan tukiasemaan. Tähän liittyen selvitin erilaisia vaihtoehtoja VPN-yhteyksien toteutuksista käyttäen nimenomaan pfSense-ohjelmistoa, koska sellainen toimii päästä-päähän VPN-tunnelin päätepisteinä myös siinä yhteydessä. Avoimen lähdekoodin pfSense, joka on reititin-palomuuri ohjelmisto, on määritelty VPN-tunnelin muodostamiseen sekä Porin että Kuopion päässä käyttämään julkista IP-osoitetta. Tämä on liikuteltavalle tukiasemalle sopimatonta, koska se vaatisi asetusten muuttamista aina kun sen sijainti muuttuu. Laboratorioverkon ylläpidon kannalta olisi edullisinta, että siirrettävän 3G-tukiaseman VPN-palvelun kiinteänä päätepisteenä on sama palvelin, kuin olemassa oleva Savonia AMK:n suuntaan, mutta toisessa päässä pitää saada käyttää lähiverkon yksityisiä IP-osoitteita DHCP:n kautta. Harkinnan jälkeen pfSense-valikoimasta valitsin openVPN-tunnelin käyttäen asiakas-palvelinarkkitehtuuria, joka tarjoaa etäpäässä dynaamista IP-osoitetta. Onnistuneiden asennusten jälkeen testattiin WAN-Bridge simulointisovelluksella pitkien etäisyyksien vaikutusta yhteyden laatuun.

Haluaisin kiittää mielekkäästä aiheesta ja rakentavista neuvoista lehtori Juha Aromaata. Kiitän myös laboratorioinsinööri Timo Viitasta sekä asiantuntija Tero Seessaloa avustuksesta matkapuhelinkeskuksen laiteasennuksissa ja sen verkkotopologian yksityiskohtien selvittelyssä.

LÄHTEET

[1] SAMK NGN-laboratorion topologiakuva. Viitattu 10.14.2015. http://samk.fi/download/28254_ngn_kuva_12112014.pdf

[2] Routing internet traffic through a site-to-site OpenVPN-connection in PfSense 2.1. Viitattu 22.10.2015. https://doc.pfsense.org/index.php/Routing_internet_traffic_through_a_site-to-site_OpenVPN-connection_in_PfSense_2.1

[3] Universal Mobile Telecommunications System (UMTS) Synchronisation in UTRAN Stage 2 (3GPP TS 25.402 version 12.1.0 Release 12). Viitattu 19.10.2015. http://www.etsi.org/deliver/etsi_ts

[4] Bannister, J., Mather, P. & Coope, S. 2004. Convergence technologies for 3G Networks : IP, UMTS, EGPRS and ATM, Chichester : John Wiley & Sons, Ltd, 2004

[5] Buechler, Ch.M. & Pringle, J. 2009. pfSense : The definitive guide to the pfSense open source firewall and router distribution, [Marysville, WA] : Reed Media Services, 2009

[6] Setting-up WAN Emulation using WAN-Bridge Live-CD v1.10. Viitattu 22.10.2015. https://code.google.com/p/wanbridge/downloads/list

[7] Holma, H. & Toskala, A. 2011. LTE for UMTS Evolution to LTE-Advanced Second Edition. Chichester : John Wiley & Sons, 2011

[8] About 3GPP. Viitattu 28.10.2015. http://www.3gpp.org/about-3gpp

[9] Mishra, Ajay R. 2010. Cellular technologies for emerging markets : 2G, 3G and beyond, Chichester : John Wiley & Sons, 2010

[10] Overview of 3GPP Release 5 V0.1.1 (2010-02). Viitattu 22.10.2015. http://www.3gpp.org/ftp/Information/WORK_PLAN/Description_Releases/Rel-05_description_20100214.zip

[11] Holma, H. & Toskala, A. 2010. WCDMA for UMTS: HSPA evolution and LTE / –5th ed. Chichester : John Wiley & Sons, 2010

[12] Nohrborg, M. LTE Overview. Viitattu 7.11.2015. http://www.3gpp.org/technologies/keywords-acronyms/98-lte

[13] OpenVPN cryptographic layer. Viitattu 11.11.2015. https://openvpn.net/index.php/open-source/documentation/security-overview.html

[14] Wannstrom, J. LTE-Advanced. Vitattu: 8.11.2015. http://www.3gpp.org/technologies/keywords-acronyms/97-lte-advanced

[15] Release 9. Viitattu 9.11.2015. http://www.3gpp.org/specifications/releases/71-release-9

[16] ITU World Radiocommunication Seminar highlights future communication technologies. 2010. Viitattu 9.11.2015. http://www.itu.int/net/pressoffice/press_releases/2010/48.aspx#.VkDhUCt401w

[17] 5G Technology Evolution Recommendations. Viitattu 11.11.2015. http://www.4gamericas.org/files/2414/4431/9312/4G_Americas_5G_Technology_Evolution_Recommendations_-_10.5.15_2.pdf

[18] Kaario, K. 2002. TCP/IP-verkot. Jyväskylä : Docendo, 2002

[19] Bertenyi, B & Flore, D. Tentative 3GPP timeline for 5G. Viitattu 11.11.2015. http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g

[20] 5G Vision. Viitattu 11.11.2015. https://5g-ppp.eu/wp-content/uploads/2015/02/5G-Vision-Brochure-v1.pdf

[21] Understanding 3GPP Release 12: Standards for HSPA+ and LTE Enhancements. Viitattu 11.11.2015. http://www.4gamericas.org/files/6614/2359/0457/4G_Americas_-_3GPP_Release_12_Executive_Summary_-_February_2015.pdf

[22] Penttinen, J. 2001. GSM-tekniikka : järjestelmän toiminta ja kehitys kohti UMTS-aikakautta. Helsinki : WSOY, 2001

[23] What distinguishes OpenVPN from other VPN packages? Viitattu 14.11.2015. http://openvpn.net/index.php/component/content/article/55.html

LIITE 1

LAITTEET JA OHJELMISTOVERSIOT

pfSense OpenVPN asiakas-palvelinarkkitehtuuri

Palvelimena toimii: Dell Optiplex 760 työasema, Intel Core2 duo CPU/4 GB RAM/160 GB HDD, kahdella Ethernet-verkkokortilla varustettuna. Asennettu ohjelmisto on pfSense 2.2.1-RELEASE (FreeBSD 10.1-RELEASE-p6)

Asiakaskoneena toimii: Dell Optiplex 755 työasema, Intel Core2 duo CPU/2 GB RAM/160 GB HDD, kahdella Ethernet-verkkokortilla varustettuna. Asennettu ohjelmisto on pfSense 2.2.1-RELEASE (FreeBSD 10.1-RELEASE-p6)

Cisco 2600 Series Router

Ohjelmistoversio 12.3

Reititin on testin aikana korvannut oikeaa Internetverkkoa. Tällä tavalla testattiin pfSense asiakas-palvelinarkkitehtuurin verkkoasetuksia ilman, että olisin käyttänyt julkista IP-osoitetta.

Verkkoemulaattori

Dell Optiplex 760 työasema, Intel Core2 duo CPU/4 GB RAM, on varustettu kahdella Ethernet-verkkokortilla. Ohjelmisto on WAN-Bridge Live-CD v1.10, USB-muistilta käynnistettynä, ilman asennuksia. WAN-Bridge sovelluksen avulla voidaan helposti jäljitellä pitkiä verkkoyhteyksiä ilman minkälaista reitityksen tarvetta.

Radioverkko-ohjain (RNC)

NSN DX200/IPA2800 alusta

Nokia WCDMA RNC ohjelmistoversio: Q 30.2-2

NGN-laboratorion laitenimi RNC5

NSN Flexi WCDMA BTS tukiasema,

ohjelmistoversio: WN6.0 22.11-187, joka koostuu kahdesta moduulista (Kuva).

Järjestelmämoduuli:

FSMD 1

Name: Flexi System Module FSMD
Product code: 471402A
Core product code: 083780A.105

Radiomoduuli:

FRGM 1
Name: FRGM Flexi RF Module 2100 Single 50 W
Product code: 471835A
Core product code: 084209A.102

Kuva. Tukiaseman radio- ja järjestelmämoduuli NGN-laboratoriossa.

<u>Puhelimet</u>

NGN-laboratorion lankapuhelimet

puhelinnumero: 02 6479902
02 6479904

ZGPAX Android watch phone S6,

käyttöjärjestelmänä Android OS v4.4

puhelinnumero: 02 6479831.

Samsung mini GT-S5570

käyttöjärjestelmänä Android OS v4.0.4

puhelinnumero: 02 6479869.

Nokia E71

puhelinnumero: 02 6479886.

PFSENSE OPENVPN-YHTEYDEN ASENNUSOHJEITA

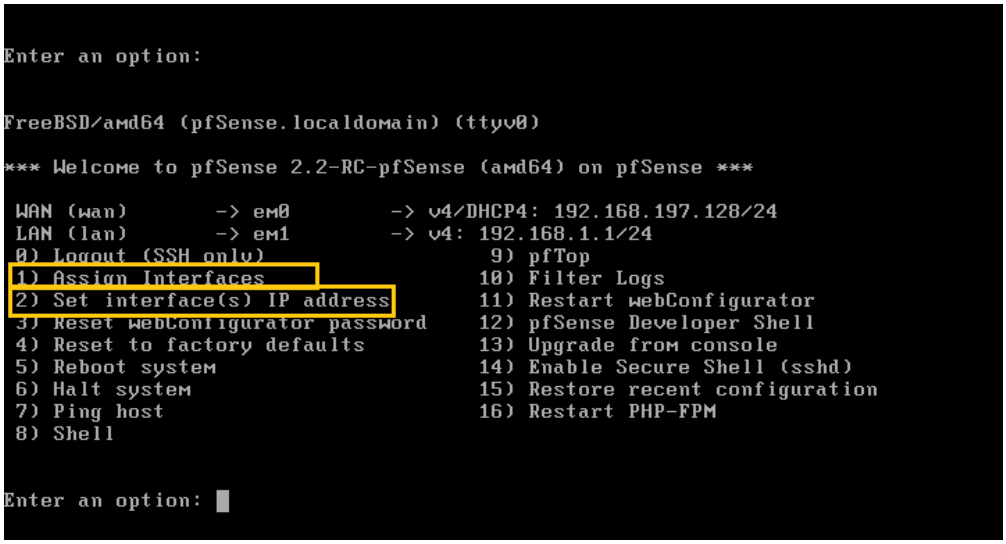
Asennusohje perustuu pfSense nettijulkaisuun: Routing internet traffic through a site-to-site OpenVPN-connection in PfSense 2.1.
https://doc.pfsense.org/index.php/Routing_internet_traffic_through_a_site-to-site_OpenVPN-connection_in_PfSense_2.1 [2]

Nimi: site-to-site, johtaa hieman harhaan jos oletetaan, että kummatkin pfSense koneet ovat kiinni Internetissä julkisilla IP-osoitteella. Kuitenkin yhteyden luonteesta johtuen, nimenomaan asiakaskone (client) voi olla myös reitittimen takana lähiverkossa, koska yhteydenotto tunnelia varten, aina lähtee asiakkaalta palvelimeen päin.

Palvelin koneen asentaminen:

Käyttöjärjestelmän asentaminen on varsin helppoa tietotekniikan ammattilaiselle. Ohjeita siihen löytyy seuraavasta linkistä:
https://doc.pfsense.org/index.php/Installing_pfSense

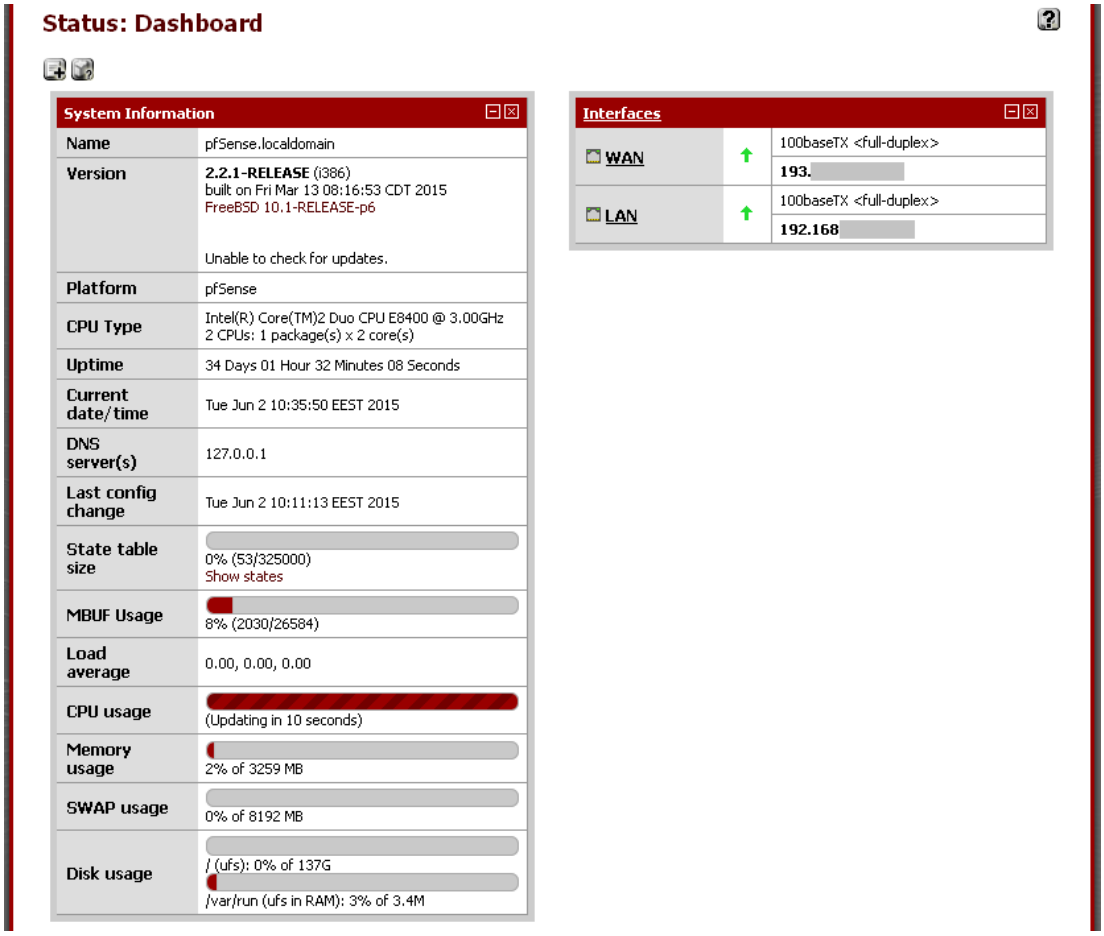
Asennuksen jälkeen pfSense käynnistyy ja pystymme valitsemaan verkkokortteja sekä määrittelemään IP-osoiteita joko manuaalisesti tai DHCP-palvelimen kautta.

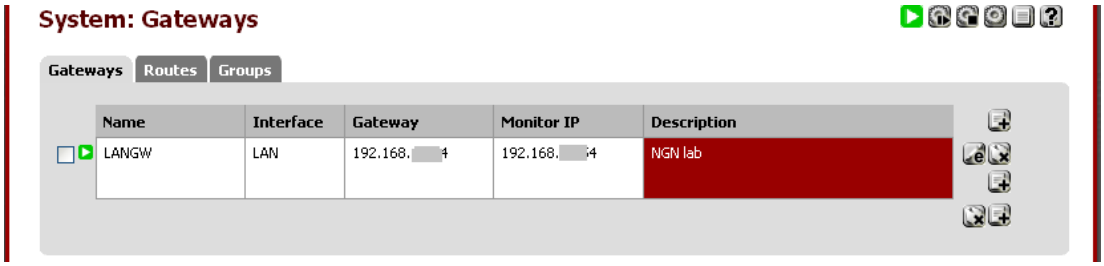


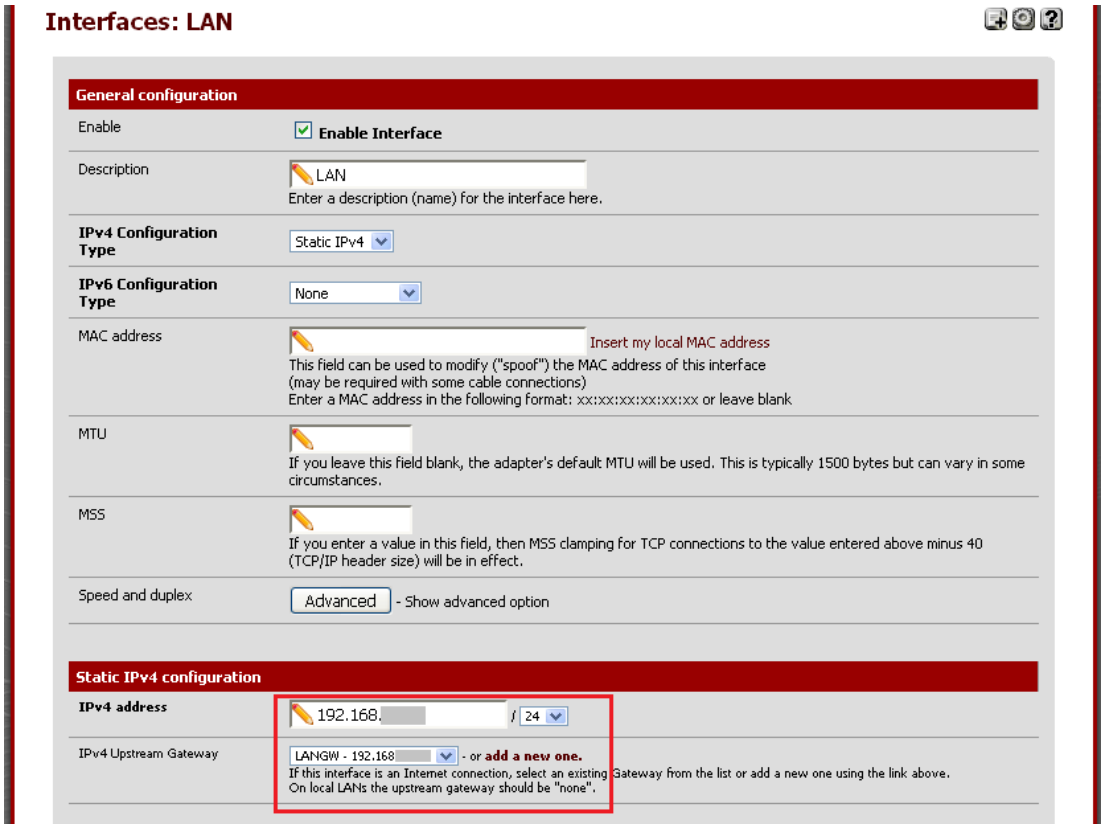
Kuva. Verkkokorttien määrittely pfSense koneella.

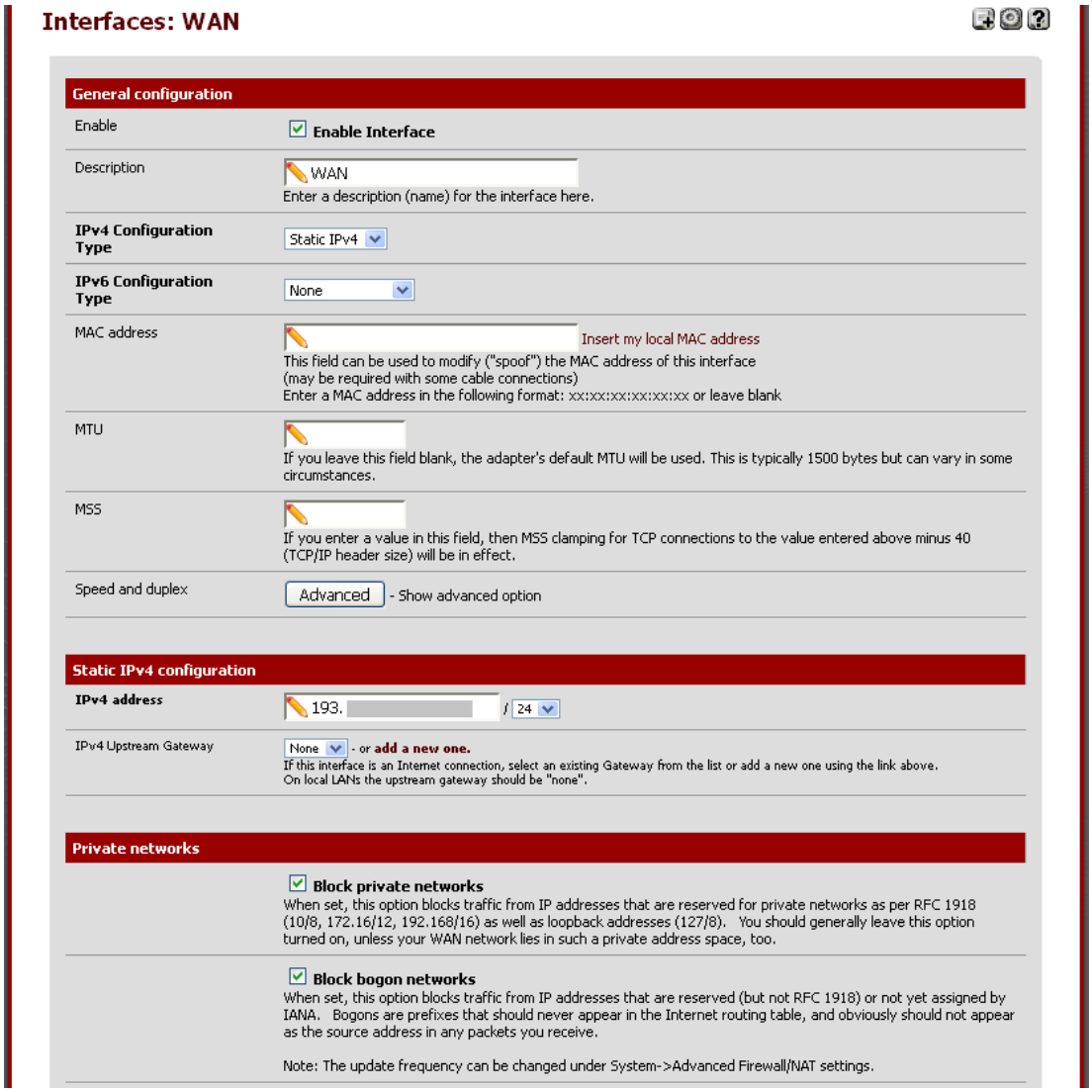
Palvelinkoneen tunnelin asetukset:

Verkkokorttien määrittelyn jälkeen selaimesta saadaan auki pfSense käyttöliittymään nimenomaan LAN-verkosta kirjautumalla oletustunnuksilla (default username *admin* and password *pfsense*). Konfigurointi on kuvien mukaisesti.






Interfaces: LAN
General configuration
Enable
Enable Interface
Description
LAN
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC address
Insert my local MAC address
This field can be used to modify ("spoof") the MAC address of this interface
(may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex
Advanced
- Show advanced option
Static IPv4 configuration
IPv4 address
192.168.
/ 24
IPv4 Upstream Gateway
LANGW - 192.168
- or add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above.
On local LANs the upstream gateway should be "none".

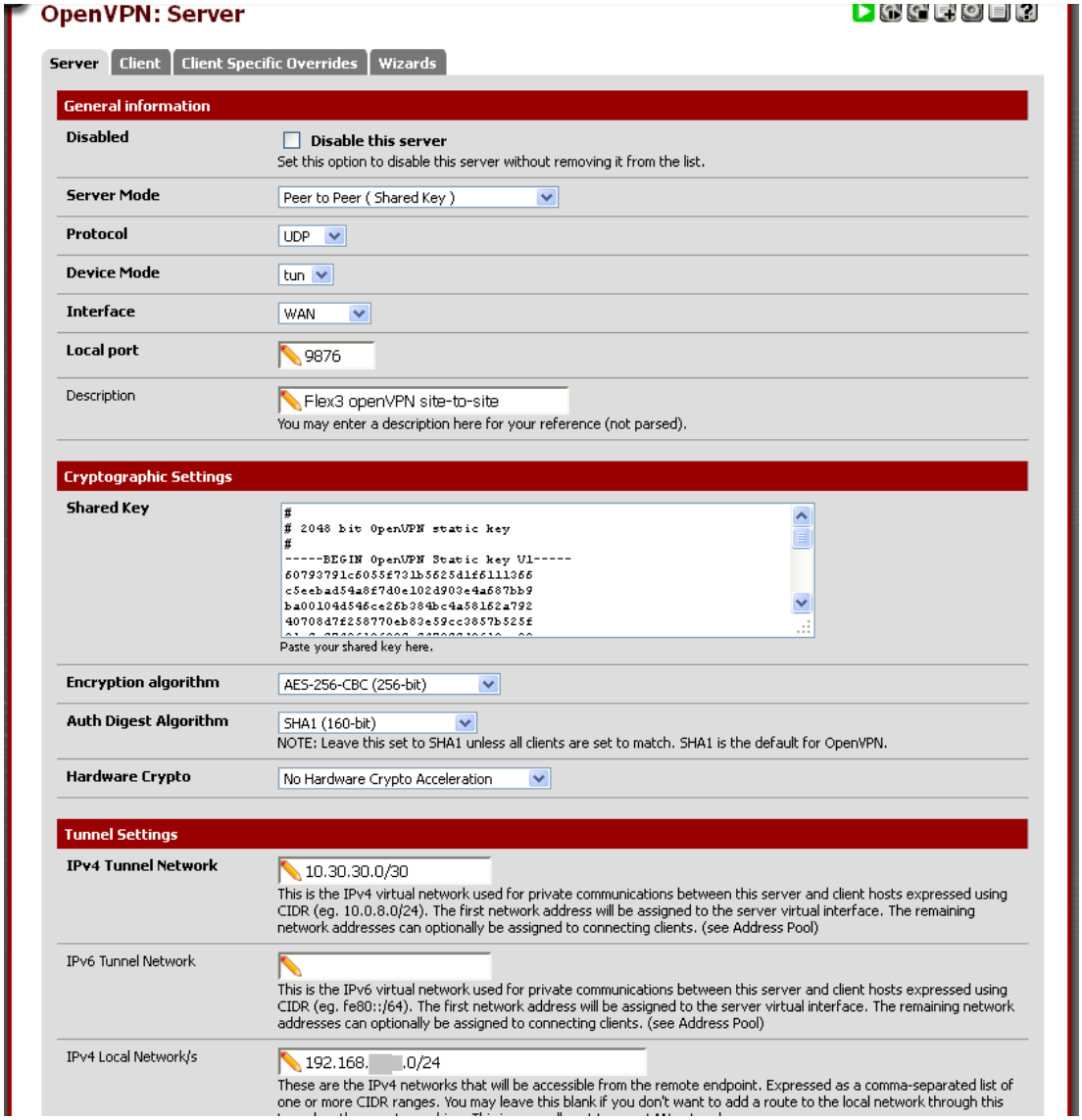


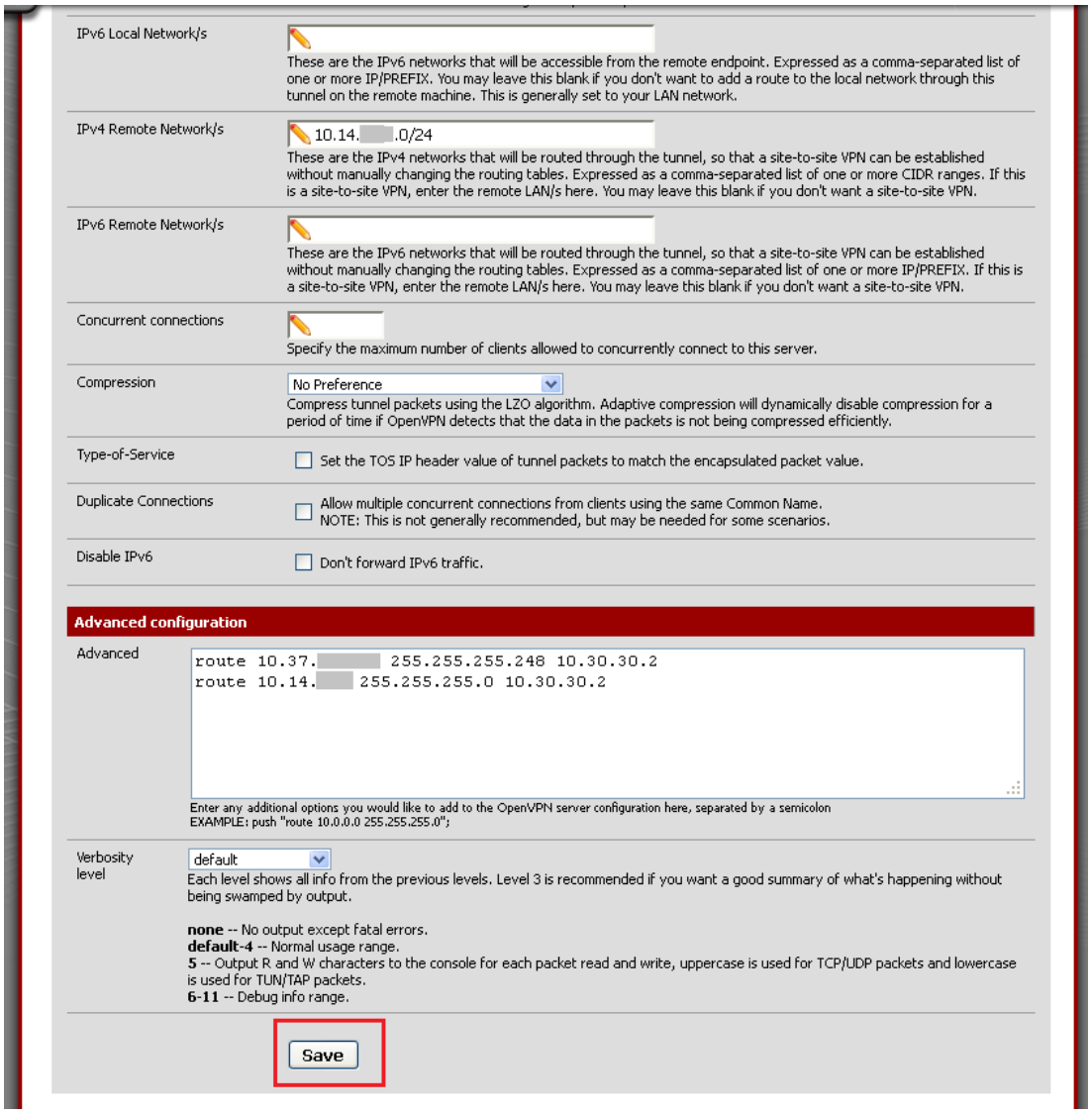
Valitse **VPN**-valikosta **OpenVPN**. **Server** välilehdessä, napsauta **+** nappulan luodaksesi uuden OpenVPN palvelimen.

Laita seuraavat asetukset:

Server Mode	Peer to Peer (Shared Key)	
Protocol	UDP	
Device Mode	tun	
Interface	WAN	
Local port	9876	1194 is the default OpenVPN port. It doesn't hurt to change it to another number to add some security through obscurity. Any unused port number may be used but we'll stick to 9876 in this article.
Description	Site-to-site	
Shared Key	Automaticly genera-ted	Copy to CLIENT
Encryption algorithm AuthDigest	AES-256-CBC (256-bit) SHA1 (160-bit)	
Hardware Crypto	No Hardware Cryp-to Acceleration un-less it is needed for this hardware.	If in doubt, select 'No Hardware Crypto Accele-ration'.
IPv4 Tunnel Network	10.30.30.0/30	Choose a subnet that's not in use in any of the current LANs. This will be used internally by OpenVPN. We're using 192.168.204.0/30 here but any private range will do. The /30 mask is because OpenVPN will only use one IP address per site. We're connecting two sites so two addresses will suffice. /24 will work but is over-kill.
IPv6 Tunnel Network	leave empty	
IPv4 Local Network/s	192.168.x.x/24	NGN laboratory's subnet
IPv6 Local Network/s	leave empty	
IPv4 Remote Network/s	10.14.x.0/24	FLEXI3's subnet
IPv6 Remote Network/s	leave empty	
Concurrent connections	leave empty	
Compression	No preference	Check if the bulk of the data transferred will be

		uncompressed data, like Office documents. Leave unchecked if the bulk is already compressed, like divx films. Routers on faster hardware can compress faster.
Type-of-Service	unchecked	
Duplicate Connections	unchecked	
Advanced	leave empty	





Status: OpenVPN

Peer to Peer Server Instance Statistics

Name	Status	Connected Since	Virtual Addr	Remote Host	Bytes Sent	Bytes Rcvd	Service
Flex3 openVPN site-to-site UDP:9876	up	Wed May 20 14:11:59 2015	10.30.30.1	193.	995.31 MB	1012.89 MB	

Firewall & NAT settings

Firewall: Rules

Floating | WAN | LAN | OpenVPN

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	RFC 1918 networks	*	*	*	*	*		Block private networks
		*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks
		IPv4 UDP	*	*	WAN address	9876	*	none		pass openVPN tunnel
		IPv4 *	*	*	*	*	*	none		allow all

Firewall: NAT: Outbound

Port Forward | 1:1 | Outbound | NPt

Mode:
- Automatic outbound NAT rule generation (IPsec passthrough included)
- Hybrid Outbound NAT rule generation (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation (No Outbound NAT rules)

Save

Mappings:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	192.168.	*	*	*	WAN address	*	NO	laboratory network

Automatic rules:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
LAN	127.0.0.0/8 10.12 /32 10.131. /26 10.130 /28 193. 0/24 10.30.30.0/30	*	*	500	LAN address	*	YES	Auto created rule for ISAKMP
LAN	127.0.0.0/8 10. /32 10.131. 2/26 10.130 /28 193 /24 10.30.30.0/30	*	*	*	LAN address	*	NO	Auto created rule

Firewall: Rules

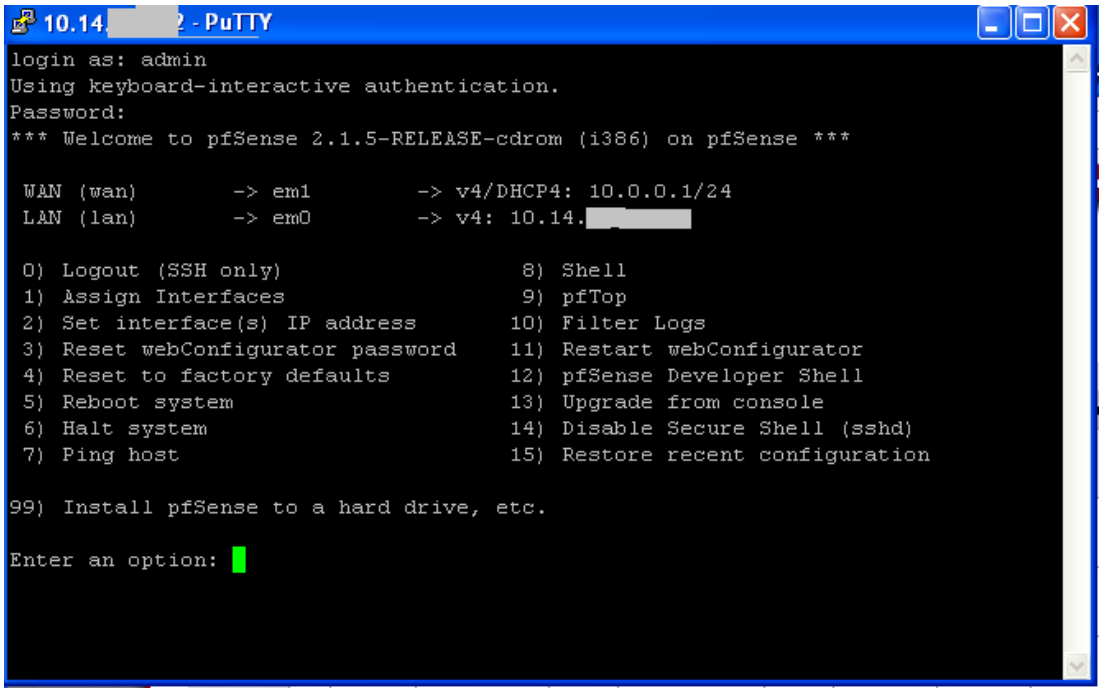
Floating | WAN | LAN | OpenVPN

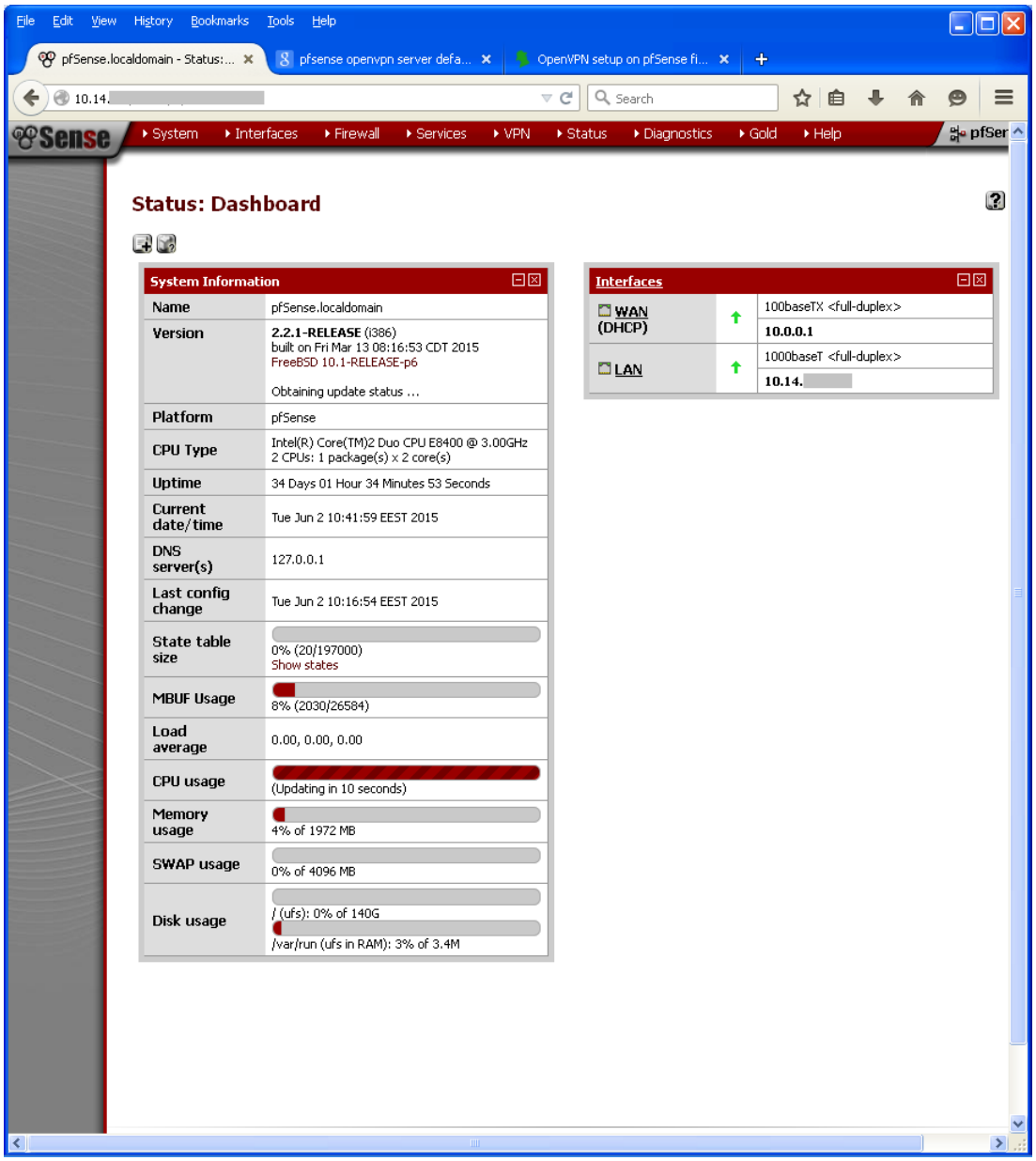
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule
		IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
		IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule
		IPv4 ICMP echoreq	10.12.	*	192.168.	*	*	none		Easy Rule: Passed from Firewall Log View
		IPv4 *	*	*	*	*	*	none		allow all

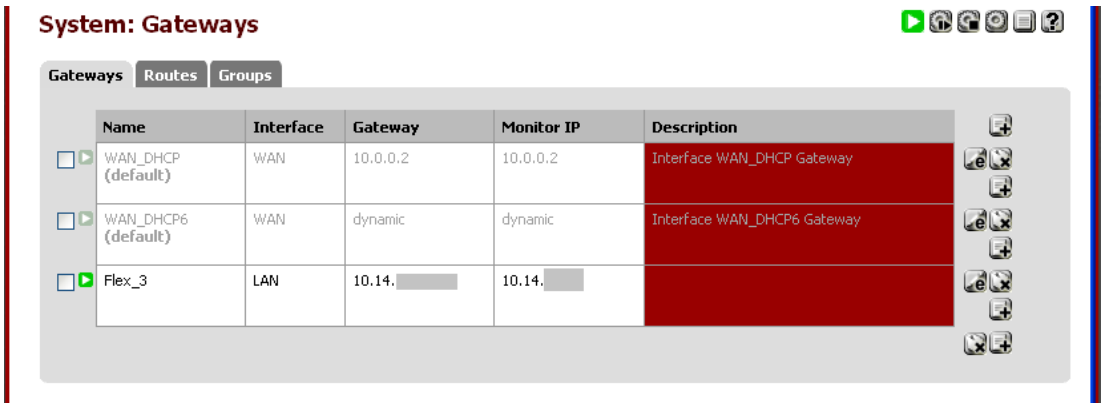
Asiakaskoneen tunnelin asetukset:

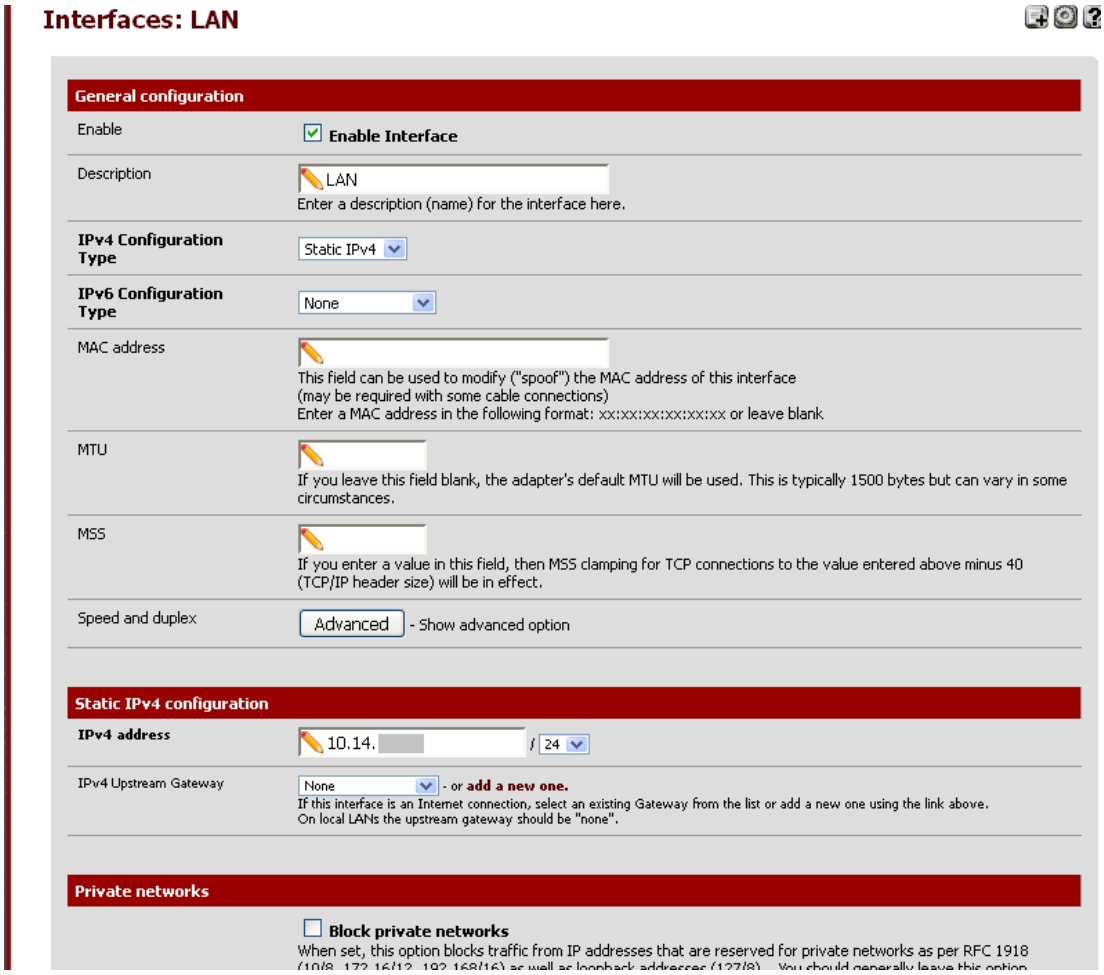
Verkkokorttien määrittelyn jälkeen selaimesta saadaan auki pfSense käyttöliittymään nimenomaan LAN-verkosta kirjautumalla oletustunnuksilla (default username *admin* and password *pfsense*).

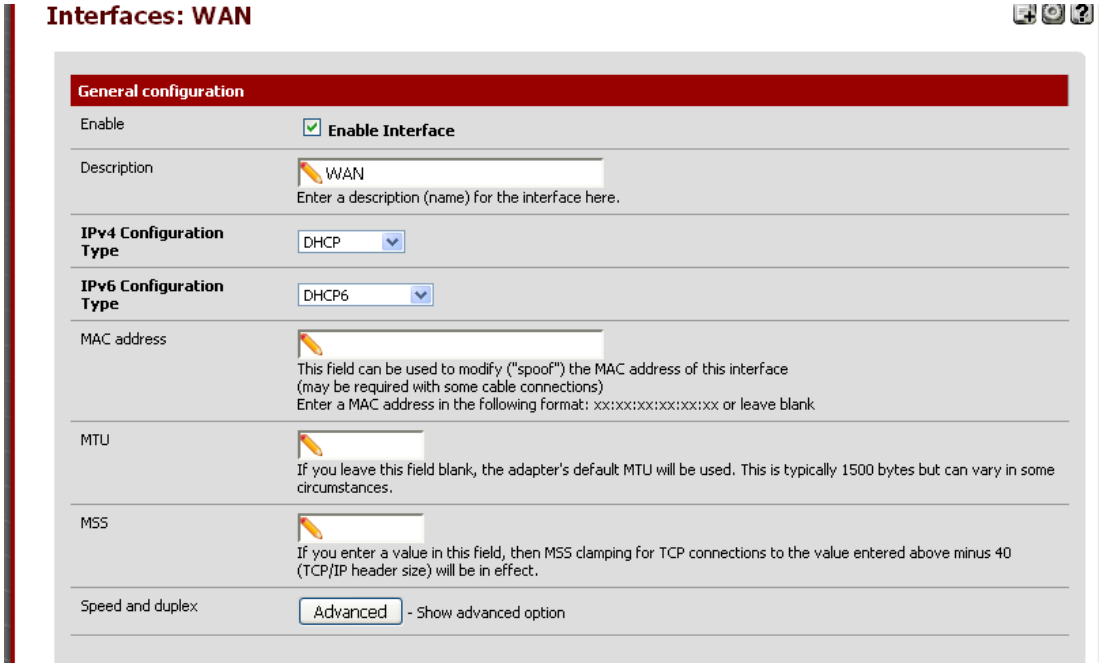
CLIENT




File Edit View History Bookmarks Tools Help
pfSense.localdomain - Status:...
pfsense openvpn server defa...
OpenVPN setup on pfSense fi...
10.14.
Search
pfSense
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
pfSer
Status: Dashboard
System Information
Name
pfSense.localdomain
Version
2.2.1-RELEASE (i386)
built on Fri Mar 13 08:16:53 CDT 2015
FreeBSD 10.1-RELEASE-p6
Obtaining update status ...
Platform
pfSense
CPU Type
Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz
2 CPUs: 1 package(s) x 2 core(s)
Uptime
34 Days 01 Hour 34 Minutes 53 Seconds
Current date/time
Tue Jun 2 10:41:59 EEST 2015
DNS server(s)
127.0.0.1
Last config change
Tue Jun 2 10:16:54 EEST 2015
State table size
0% (20/197000)
Show states
MBUF Usage
8% (2030/26584)
Load average
0.00, 0.00, 0.00
CPU usage
(Updating in 10 seconds)
Memory usage
4% of 1972 MB
SWAP usage
0% of 4096 MB
Disk usage
/ (ufs): 0% of 140G
/var/run (ufs in RAM): 3% of 3.4M
Interfaces
WAN (DHCP)
100baseTX <full-duplex>
10.0.0.1
LAN
1000baseT <full-duplex>
10.14.


System: Gateways
Gateways
Routes
Groups
Name
Interface
Gateway
Monitor IP
Description
WAN_DHCP (default)
WAN
10.0.0.2
10.0.0.2
Interface WAN_DHCP Gateway
WAN_DHCP6 (default)
WAN
dynamic
dynamic
Interface WAN_DHCP6 Gateway
Flex_3
LAN
10.14.
10.14.


Interfaces: LAN
General configuration
Enable
Enable Interface
Description
LAN
Enter a description (name) for the interface here.
IPv4 Configuration Type
Static IPv4
IPv6 Configuration Type
None
MAC address
This field can be used to modify ("spoof") the MAC address of this interface
(may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex
Advanced
- Show advanced option
Static IPv4 configuration
IPv4 address
10.14.
/ 24
IPv4 Upstream Gateway
None
- or add a new one.
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the link above.
On local LANs the upstream gateway should be "none".
Private networks
Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918


Interfaces: WAN
General configuration
Enable
Enable Interface
Description
WAN
Enter a description (name) for the interface here.
IPv4 Configuration Type
DHCP
IPv6 Configuration Type
DHCP6
MAC address
This field can be used to modify ("spoof") the MAC address of this interface
(may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank
MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.
Speed and duplex
Advanced
- Show advanced option

Firewall: NAT: Outbound

Port Forward | 1:1 | Outbound | NPt

Mode:
- Automatic outbound NAT rule generation (IPsec passthrough included)
- Hybrid Outbound NAT rule generation (Automatic Outbound NAT + rules below)
- Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)
- Disable Outbound NAT rule generation (No Outbound NAT rules)

Save

Mappings:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description

Automatic rules:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
WAN	127.0.0.0/8 10.37. /29 10.14 /24 10.30.30.0/30	*	*	500	WAN address	*	YES	Auto created rule for ISAKMP
WAN	127.0.0.0/8 10.37. /29 10.14. /24 10.30.30.0/30	*	*	*	WAN address	*	NO	Auto created rule

Firewall: Rules

Floating | WAN | LAN | OpenVPN

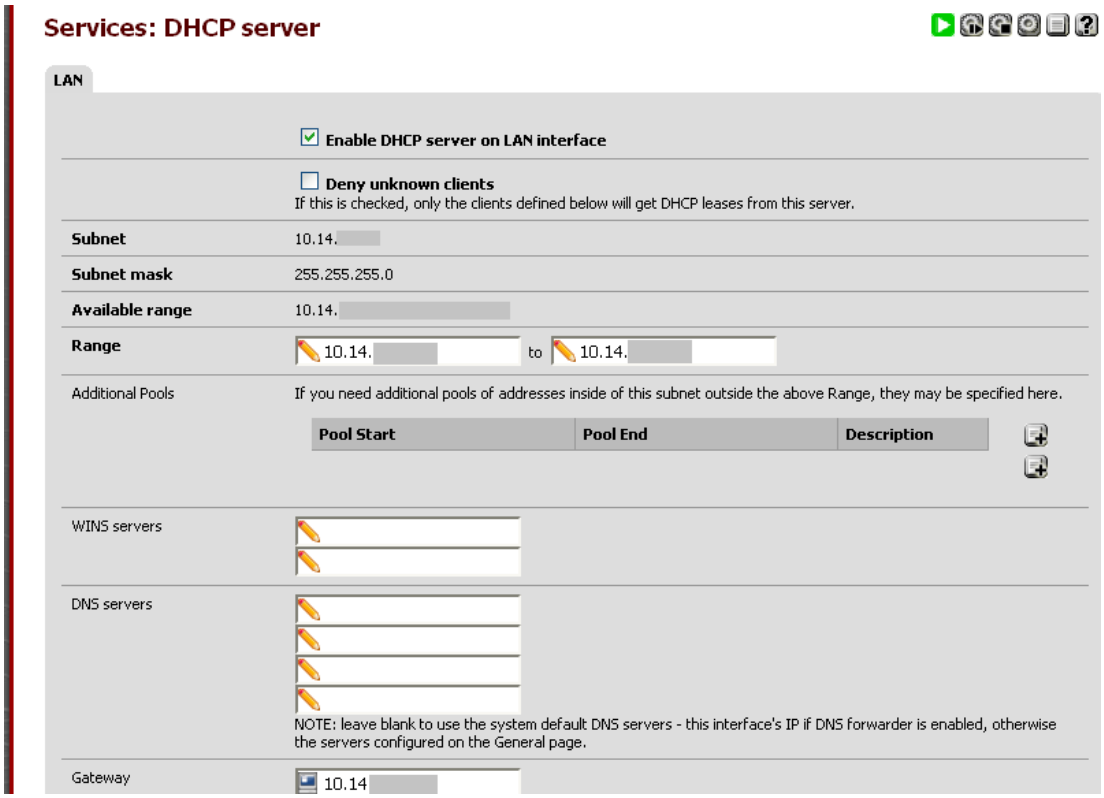
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	*	*	*	LAN Address	80 22	*	*		Anti-Lockout Rule
	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule
	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule
	IPv4 UDP	10.37. /29	*	*	*	*	none		allow from Flex3 BTS & TRS
	IPv4 ICMP echoreq	10.37.	*	10.14.	*	*	none		Easy Rule: Passed from Firewall Log View
	IPv4 TCP	10.37.	*	192.168.	*	*	none		Easy Rule: Passed from Firewall Log View
	IPv4 ICMP echoreq	*	*	*	*	*	none		Easy Rule: Passed from Firewall Log View
	IPv4 *	*	*	*	*	*	none		allow all

Firewall: Rules

Floating | WAN | LAN | OpenVPN

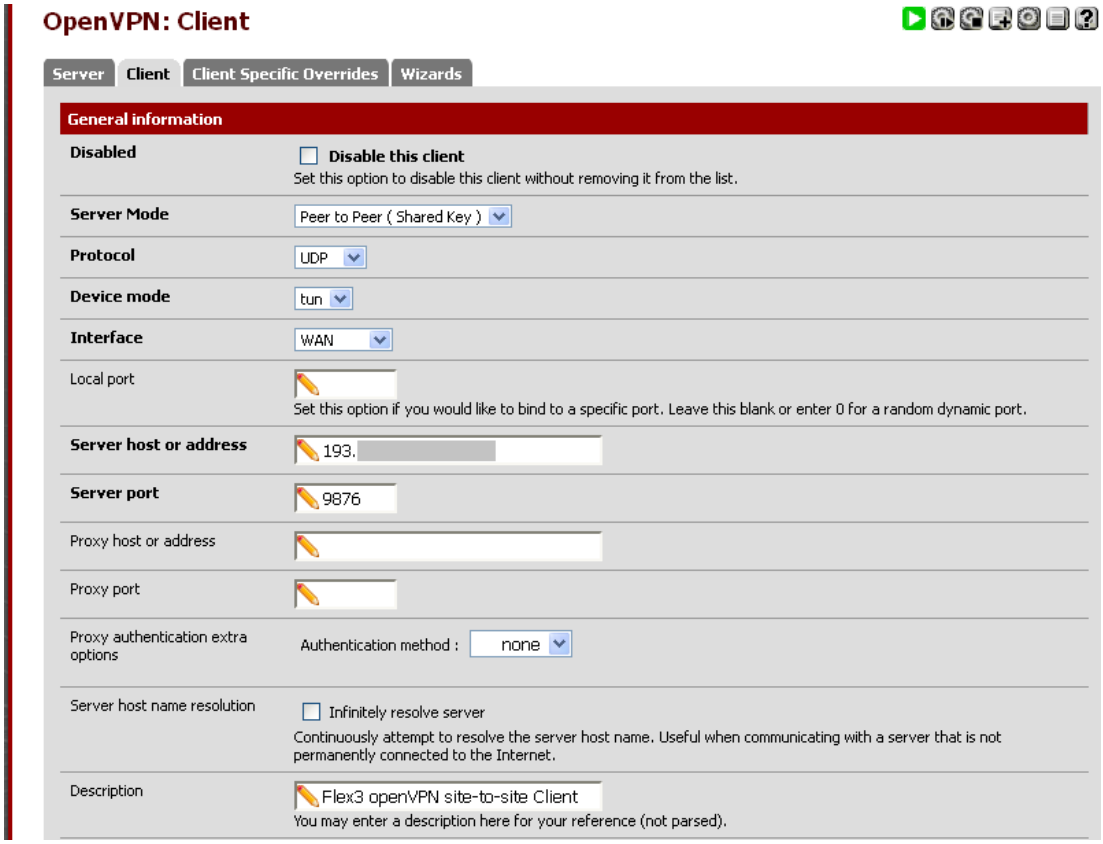
ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	IPv4 ICMP echoreq	10.30.30.1	*	10.14.	*	*	none		Easy Rule: Passed from Firewall Log View
	IPv4 *	*	*	*	*	*	none		allow everything through openVPN

DHCP-palvelu tarjoaa etäpäässä mahdollisuutta kytkemään tietokoneen tukiaseman verkkoon ja sitä voidaan käyttää konfigurointiin.

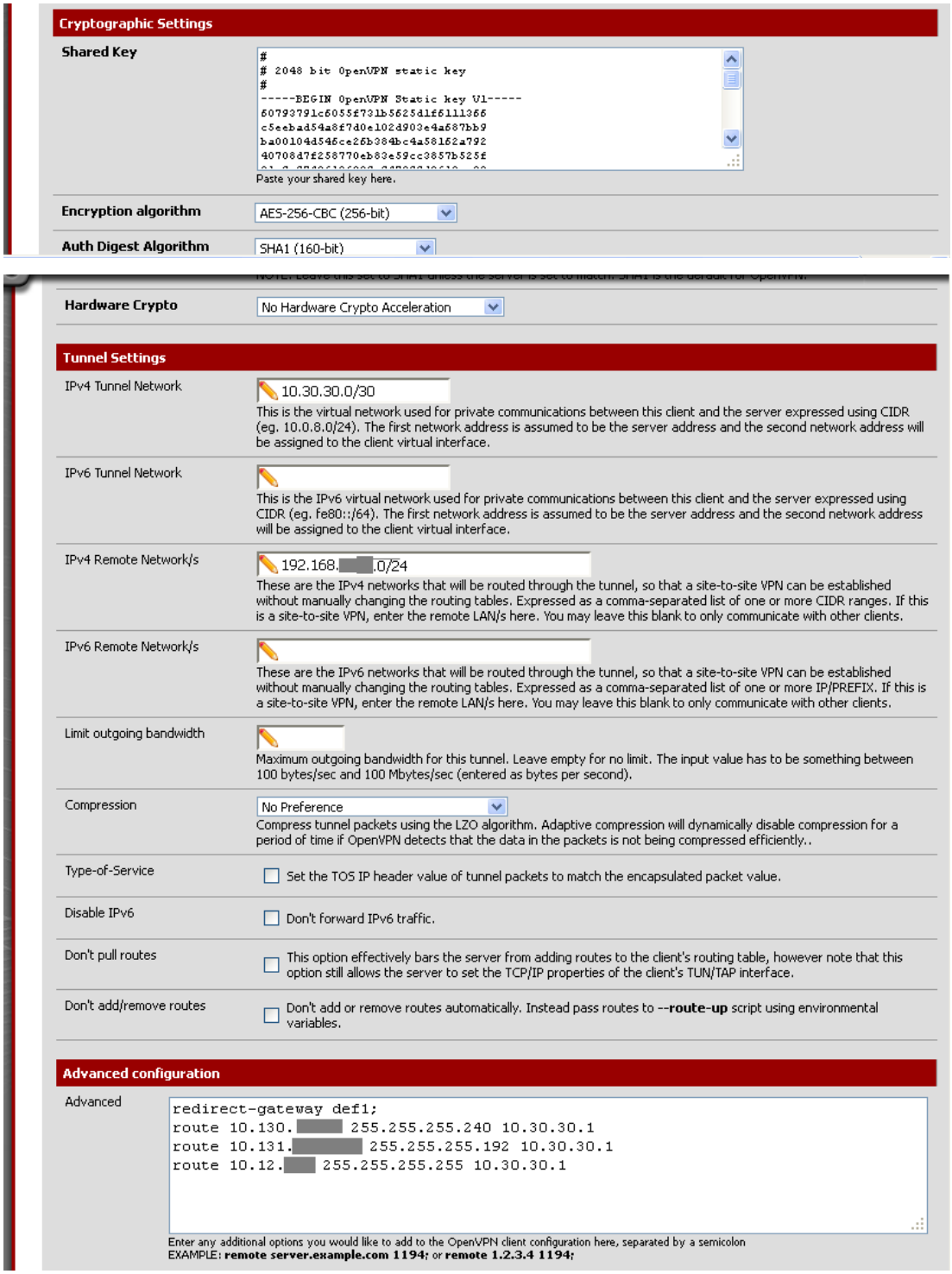


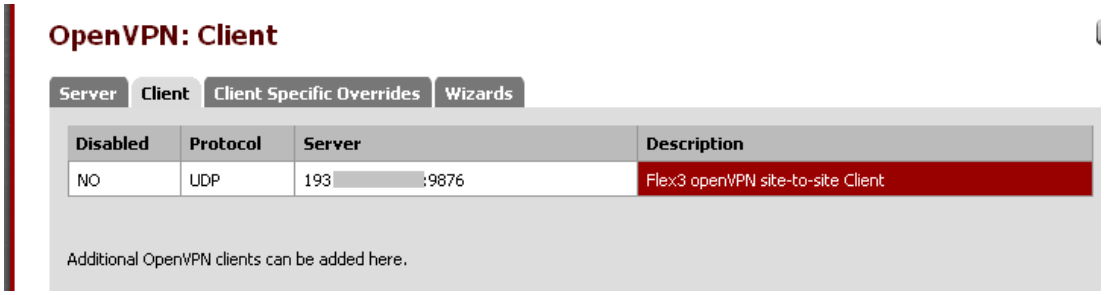
Disabled	not checked	
Server Mode	Peer to Peer (Shared Key)	
Protocol	UDP	same as Site B
Device mode	tun	
Interface	WAN	
Local port	leave empty	
Server host or address	193.x.x.x	IP address or FQDN
Server port	9876	the port Site B is running the OpenVPN server on
Proxy host or address	leave empty if not using a proxy	
Proxy port	leave empty if not using a proxy	
Proxy authentication extra options	leave empty if not using a proxy	
Server host name resolution	check if Site B sometimes has connectivity problems	
Shared Key	do not check ‘Automatically generate a	

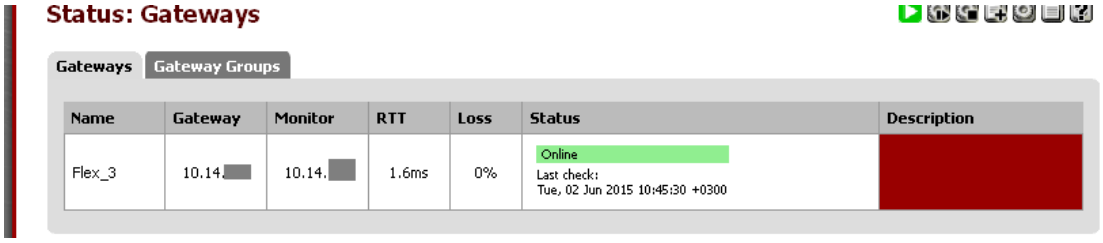
	shared key' but paste the Shared Key from openVPN-server	
Encryption algorithem	AES-256-CBC (256-bit)	same as Site B
Hardware Crypto	Choose 'No Hardware Crypto Acceleration' unless the hardware has an accelerator	
IPv4 Tunnel Network	10.30.30.0/30	same as Site B
IPv6 Tunnel Network	leave empty	
IPv4 Remote Network/s	192.168.x.0/24	site A's subnet
IPv6 Remote Network/s	leave empty	
Limit outgoing bandwidth	leave empty unless required	
Compression	No preference	
Type-of-Service	not checked	
Advanced		



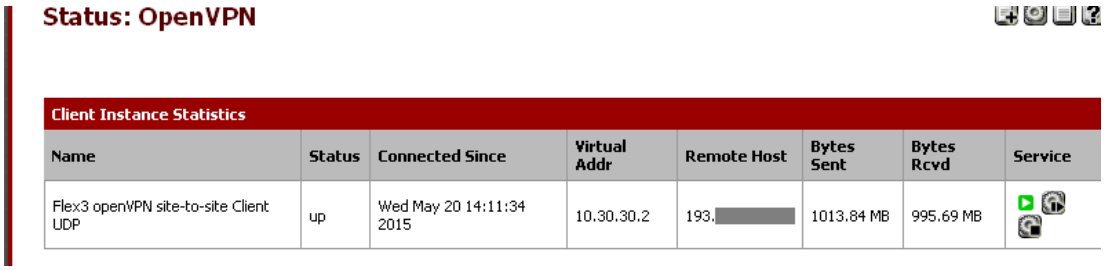
Salausavain pitää olla sama kuin openVPN-palvelimessa.



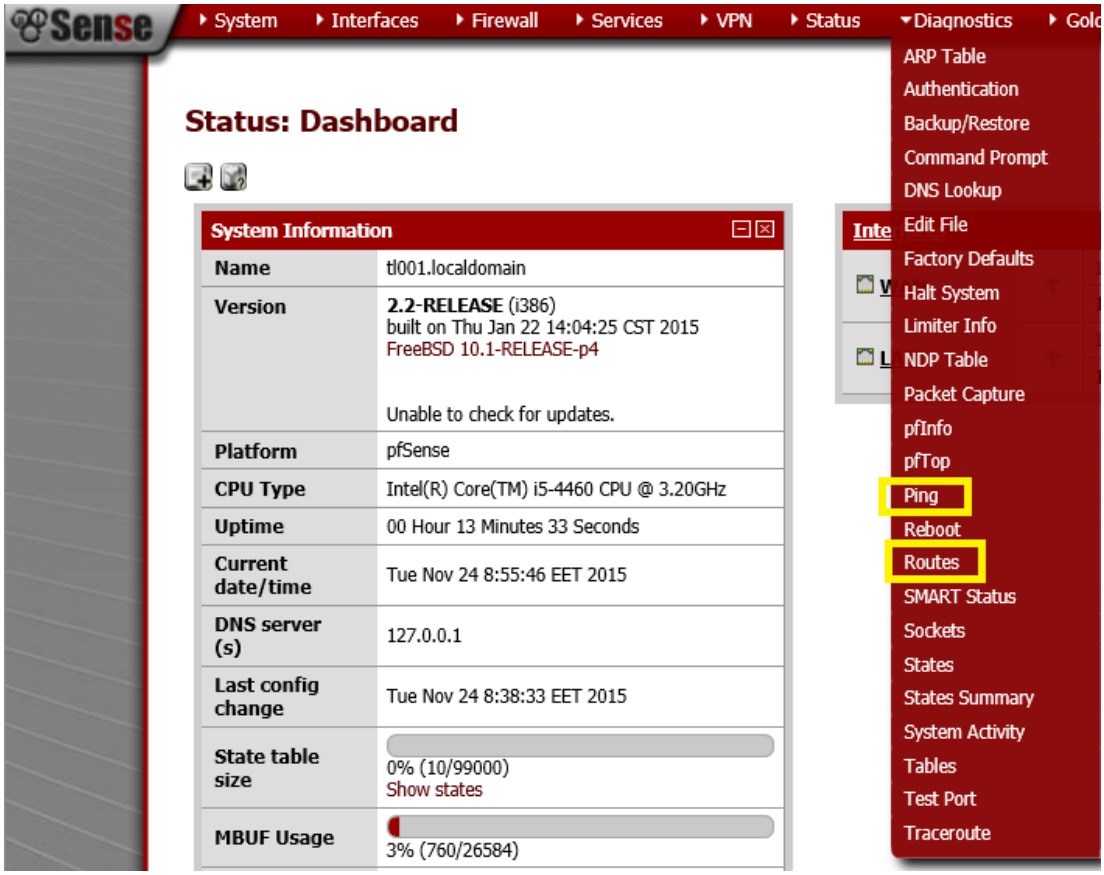


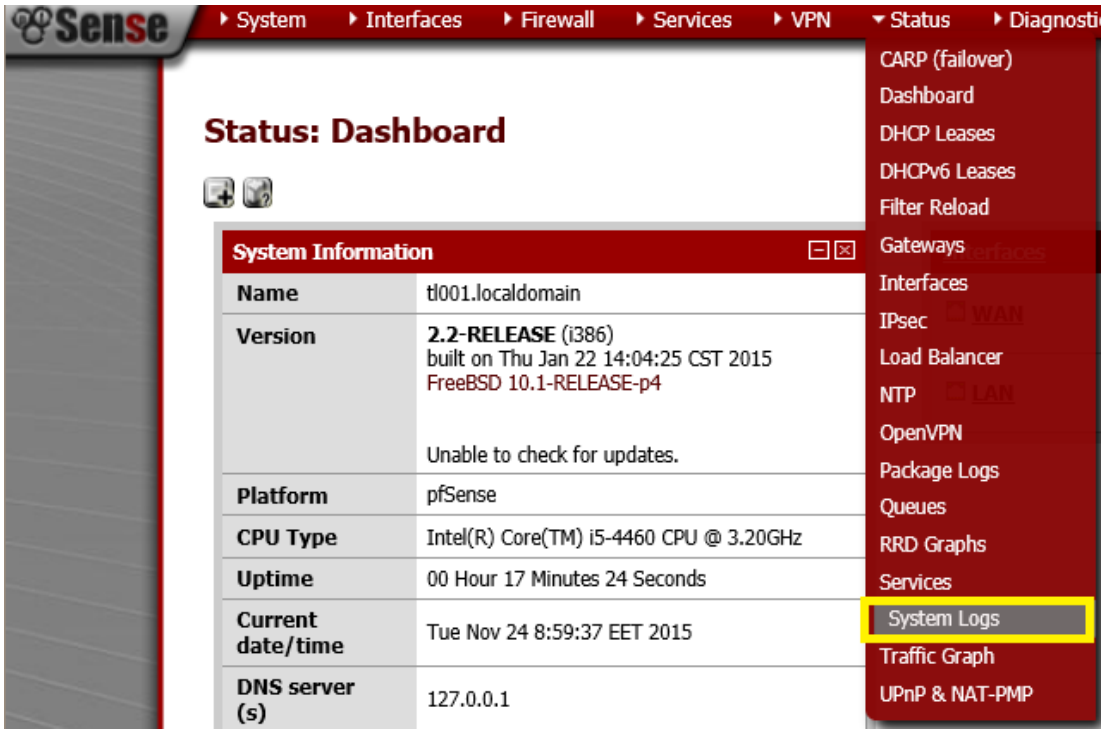


Jos kaikki asennettu oikein, openVPN-tunnelin tilanne on tämän kaltainen.

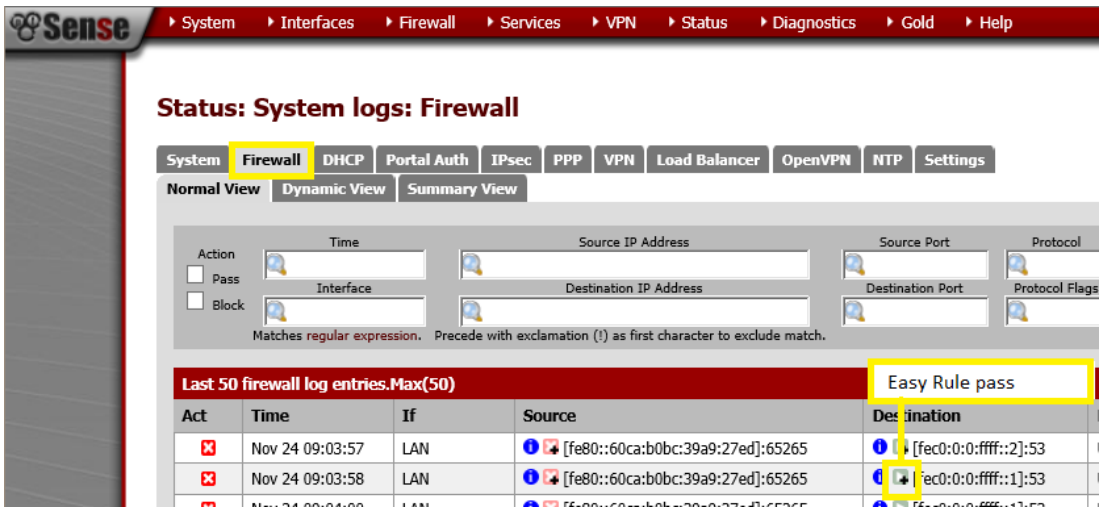


<u>Vikojen selvittelyyn käytetään pfSense-työkaluja:</u>




System
Interfaces
Firewall
Services
VPN
Status
Diagnosti
CARP (failover)
Dashboard
DHCP Leases
DHCPv6 Leases
Filter Reload
Gateways
Interfaces
IPsec
Load Balancer
NTP
OpenVPN
Package Logs
Queues
RRD Graphs
Services
System Logs
Traffic Graph
UPnP & NAT-PMP
Status: Dashboard
System Information
Name
tl001.localdomain
Version
2.2-RELEASE (i386)
built on Thu Jan 22 14:04:25 CST 2015
FreeBSD 10.1-RELEASE-p4
Unable to check for updates.
Platform
pfSense
CPU Type
Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz
Uptime
00 Hour 17 Minutes 24 Seconds
Current date/time
Tue Nov 24 8:59:37 EET 2015
DNS server (s)
127.0.0.1


System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Status: System logs: OpenVPN
System
Firewall
DHCP
Portal Auth
IPsec
PPP
VPN
Load Balancer
OpenVPN
NTP
Last 50 OpenVPN log entries
Nov 21 10:34:27
openvpn[48974]: Authenticate/Decrypt packet error: packet HMAC authentication failed


System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Gold
Help
Status: System logs: Firewall
System
Firewall
DHCP
Portal Auth
IPsec
PPP
VPN
Load Balancer
OpenVPN
NTP
Settings
Normal View
Dynamic View
Summary View
Action
Pass
Block
Time
Source IP Address
Source Port
Protocol
Interface
Destination IP Address
Destination Port
Protocol Flags
Matches regular expression.
Precede with exclamation (!) as first character to exclude match.
Last 50 firewall log entries.Max(50)
Easy Rule pass
Act
Time
If
Source
Destination
Nov 24 09:03:57
LAN
[fe80::60ca:b0bc:39a9:27ed]:65265
[fec0:0:0:ffff::2]:53
Nov 24 09:03:58
LAN
[fe80::60ca:b0bc:39a9:27ed]:65265